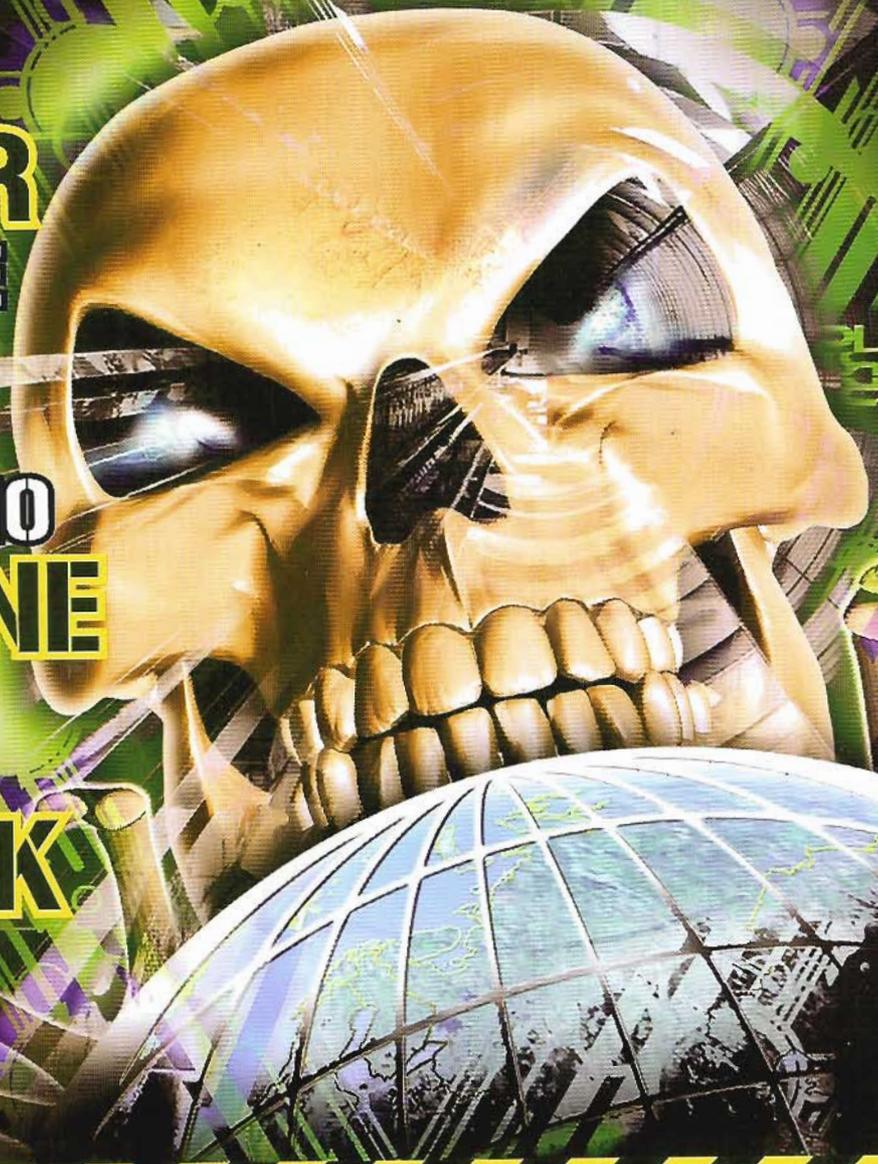
TUTTO QUELLO CHE GLI ALTRI NON DICONO
NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2 €
HACKER JOURNAL
n.192
www.hackerjournal.it
EMULE
I VAMPIRI DELLA RETE
SCUOLA HACKER
KEYLOGGER
SPIE PEREFETTE
MOBILE
SINCRONIZZIAMO
PC & IPHONE
SNIFFING
WIRESHARK
IL CACCIATORE
FOCUS ON
DEFT LINUX
CSI FILE_RECUPERO TOTALE
QUATTORD. ANNO 10 - Nº 192 - 7/20 GENNAIO 2010 - € 2,00
WLF PUBLISHING

Anno 10 – N.192
7 gennaio / 20 gennaio 2010

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

Anno nuovo vita nuova

"Anche la bestia più feroce conosce un minimo di pietà. Ma io non ne conosco, perciò non sono una bestia."
(William Shakespeare)

Il 2009 è finito, carico di polemiche che ci hanno visti sulla bocca di tutti, i cattivi in prima linea, quelli da mettere alla gogna, la causa di tutti i mali e dei fatti di cronaca che hanno visto il Primo Ministro vittima di una mano mossa da siti Web carichi di odio. Ma non siamo noi. Non siamo quelli e non lo siamo mai stati. La recrudescenza degli attacchi ai siti istituzionali, quello di Poste Italiane su tutti, sembrava fatta apposta per giustificare il decreto legge Maroni, che ha portato l'ennesimo giro di vite stringendo le maglie già strette della nostra libertà intellettuale di internauti liberi.

Adesso basta, è venuto il momento di prendere le distanze. Hacker è filosofia di vita, Hacker è poesia e pensiero, hacker è curiosità, Hacker è consapevolezza, Hacker è rispetto.

Strumentalizzarci, accostare la nostra filosofia a dei ragazzini che giocano sul Web spaccando tutto ciò che incontrano sulla propria strada, è quanto di più scontato e scorretto possa esserci. Non siamo noi. Non ci interessa la politica, non ci interessa attaccare, non ci interessa la violenza, non ci interessa l'ignoranza ottusa. Noi siamo quelli curiosi, quelli rispettosi, che vogliono migliorare le cose per il gusto di farlo, perchè se possono andar meglio è giusto che ci vadano.

La strada è lunga, ma abbiamo a disposizione un anno nuovo per farne un altro pezzetto. Il nostro nome non ne uscirà riabilitato, ma noi sappiamo... che non siamo noi quelli cattivi! Buon Anno Hacker!!!

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ: mandateci una mail!
Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa.
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Freni al Grande Fratello

Non stiamo parlando della trasmissione televisiva: quella, purtroppo, continua a occupare spazi che potrebbero benissimo essere dedicati a qualcosa di più intelligente. Parliamo invece delle nuove norme che vanno ad adeguare il regolamento in fatto di videosorveglianza, in particolar modo per quanto riguarda i dispositivi di sicurezza messi in atto da molti comuni italiani. Si fa presto, infatti, a dire "piazzo una telecamera qui e una laggiù": chi avrà accesso poi alle immagini registrate da queste telecamere?

Finora, le norme esistenti si basavano sulle tecnologie e sulle loro possibilità disponibili all'atto della stesura del regolamento precedente. Ma siamo in un ambito in cui lo sviluppo tecnologico è stato rapidissimo, è naturale quindi che al giorno d'oggi qualcosa debba essere ritoccato. La cosa consolante è, per quanto riguarda noi comuni cittadini, che le nuove regole vanno a toccare solamente i comuni e gli organi di sicurezza: non più quindi spionaggio indiscriminato della vita comunitaria del nostro paese, ma paletti ben piazzati per fare in modo che le nostre vite appartengano solo a noi e a nessun altro. Limitato quindi il tempo di conservazione delle immagini registrate, limitato l'accesso alle stesse solamente a quei membri delle forze dell'ordine che devono usarle solo con finalità di indagine per la verifica di potenziali reati, accessibilità della documentazione multimediale per tutti i cittadini che si vedono recapitare una contravvenzione per una violazione del codice stradale e il divieto di riprendere le nostre targhe automobilistiche se non in caso di accertata violazione del codice da parte nostra. In più, i comuni che fanno uso di sistemi di videosorveglianza dovranno segnalarlo attraverso indicazioni luminose a tutti i cittadini. Salatissime le multe per i comuni che non si adeguano: fino a 120.000 euro per chi non sottopone le necessarie richieste al Garante della Privacy, fino a 180.000 euro per chi invece non modifica i propri comportamenti in violazione delle nuove norme, che possono anche essere quadruplicati. Tutto bene, o quasi: ci chiediamo come faranno i comuni eventualmente multati per una violazione a recuperare i soldi necessari per pagare. Non stupiamoci se, di punto in bianco, ci vedremo recapitare un bollettino per una nuova tassa comunale sul possesso di scarpe da tennis: probabilmente il comune ha curiosato troppo nelle nostre vite...

TOTTI AFFONDATO?

Il nuovo sito del capitano della Roma è stato oggetto di un attacco Hacker, almeno così afferma il Francesco nazionale proprio dalle pagine di www.francescototti.com. La nuova veste grafica ha attirato migliaia di visitatori, poco più di 73 mila in una sola giornata, ma subito dopo è stato oggetto di un tentativo di brute force. Fortunatamente, sempre secondo quanto afferma il capitano, i sistemi di difesa da questo tipo di attacchi hanno funzionato e il sito è stato immediatamente messo off-line per preservare l'integrtità dei dati. Niente danni quindi, nulla è stato perso e tra qualche giorno il capitano giallorosso tornerà a far bella mostra di sè anche sul Web. Sarà effettivamente così? Qualche dubbio naturalmente ci sorge, basti il fatto che dopo tre giorni dal presunto tentativo di attacco il sito risulta più morto che mai: d'altra parte Totti in difesa non è mai stato un mostro!

MAIL RUBATE: IPCC MENTE

Jean-Pascal Von Ypersele, climatologo del gruppo ONU per lo studio sui cambiamenti climatici (Ipcc), ha avuto non poche gatte da pelare in occasione del recente vertice sul clima di Copenagen che vedeva i grandi della terra seduti al tavolo per cercare contromisure al riscaldamento globale causato dall'uomo. Quache settimana fa infatti, alcune email di climatologi e fisici dell'Università di East Anglia sono state rubate e diffuse. il contenuto della corrispondenza hackerata è imbarazzante: il climatologi avrebbero volutamente ingigantito i dati sull'inquinamento per rendere più credibili la tesi dei danni dovuti all'effetto serra. Una magra figura insomma, resa possibile dal lavoro certosino di alcuni hacker gentiluomini che hanno reso pubbliche le email dello scandalo e si sono dileguati senza troppo rumore. O quasi: secondo il Mail on Sunday, infatti, avrebbero lasciato tracce inequivocabili che indicherebbero gli autori come i "famosi" hacker di Tomsk, gli stessi che nel 2002 hanno oscurato, su mandato dei servizi segreti russi, il portale di informazioni che diffondeva notizie scoomode su ciò che stava accadendo in Cecenia. C'è dietro la solita manovra politica dell'inossidabile nuovo KGB?

CHINA MOST WANTED

La Cina continua imperterrita la sua campagna contro la volgarità diffusa a mezzo Internet e con dispositivi mobili, arrivando a promuovere e remunerare la delazione. Come nel migliore dei film western, l'agenzia di controllo dei contenuti dei siti Internet cinese ha messo una taglia su tutti quei siti che pubblicizzano materiale osceno, fossero anche foto di ragazze vestite in pose ammiccanti. La taglia oscilla tra i 1000 e i 10.000 yuan (100 e 1.000 euro) a seconda dei contenuti censurabili e viene pagata solo a sito bloccato e responsabili denunciati. Ma la manovra non finisce qui: già oscurati o censurati i più importanti tracker Torrent come BTChina, i maggiori motori di ricerca liberamente (o quasi) operanti adotteranno una serie di filtri per accondiscendere alla volontà del governo e bloccare la diffusione di materiale osceno. Tra questi, Yahoo! China, Sohu e Sina, che per paura di sanzioni (o peggio) vogliono mettersi in regola entro il marzo 2010. Ciononostante i bilanci delle società legate ad Internet lievitano.

HOT NEWS

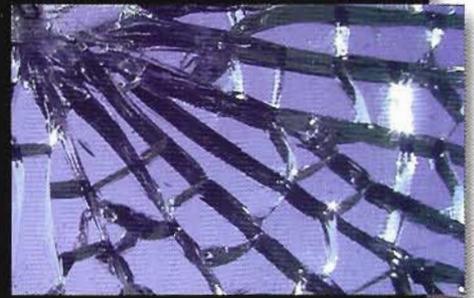
WEB TAX: LA SIAE DICE SI

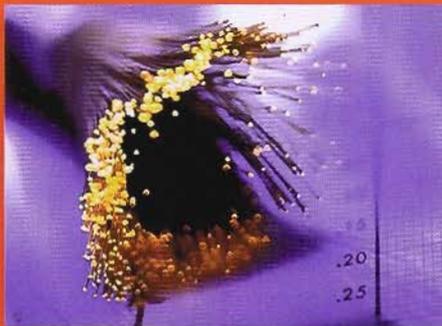
Siamo alla frutta: come se non pagassimo già abbastanza per il poco che abbiamo e il molto che non abbiamo, dalla rigidissima Germania arriva una nuova gabella: la Web Tax. Al momento è solo una proposta, che però non ha motivi per essere bocciata. In sostanza presto i cittadini teutonici dovranno pagare 17,98 euro al mese (tanto quanto il canone TV) per utilizzare Internet su computer e Smartphone. La legge prevede due proposte di pagamento: nella prima pagherebbe solo chi effettivamente usa il Web, la seconda invece propone che ogni cittadino paghi il dazio, sia che possegga una radio sia che abbia trenta PC connessi ad Internet. La SIAE ha subito raccolto l'idea lanciando una proposta analoga ora al vaglio del Ministero dei Beni Culturali: un pagamento di 2,5 euro per ogni apparecchio atto a duplicare contenuti multimediali, dal telefonino alla chiavetta USB.

PROCESSORE INTEL DA 48 CORE

Prima o poi ci si doveva arrivare, a Intel va il premio velocità 2010: il processore 48 core è già una realtà. Il primo prototipo è stato messo a punto e dopo mesi di lavoro certosino i tecnici della casa di Santa Clara annunciano l'imminente messa in produzione di quello che sarà il più potente processore singolo mai prodotto finora La data ufficiale in cui sarà in vendita non è stata ancora resa nota, ma il superprocessore in oggetto è già in funzione e pare anche che funzioni molto bene: è costruito in tecnologia a 45 nanometri, supporta fino a 64 GB di memoria RAM ed è costituito da singoli core non più potenti di un normale Atom, che però congiuntamente fanno impallidire qualunque altro processore attualmente in commercio. Il consumo previsto va dai 25 ai 125 Watt, in quanto i singoli core possono essere spenti secondo le necessità per risparmiare energia. Per curiosità, questo processore ha fatto girare senza problemi sia Windows sia Linux: da leccarsi i baffi!

NEWS DA CUPERTINO

Gioie e dolori per Apple: i nuovi iMac da 27 pollici hanno fatto fare una magra figura a Steve Jobs & Company. Monitor scheggiati agli angoli e schede grafiche ATI col mal di pancia stanno facendo ritardare in tutto il mondo la consegna del prodotto. Un duro colpo per la Mela, proprio sotto Natale: tutte le consegne sono state slittate di due settimane per ovviare al problema. Sul fronte mobile, invece, i dolori saranno per i clienti indisciplinati. Apple infatti ha depositato un brevetto che riguarda un dispositivo anti effrazione che, installato in iPod e iPhone, permette ai tecnici di scoprire se l'apparecchio è stato manomesso. Di cosa si tratta? Un banale adesivo interno che si rompe in caso di apertura. Ma quante ne sanno?

Telecom e la banda larga

Ci risiamo, periodicamente la notizia ormai riscaldata più e più volte come il peggiore dei minestroni torna a tenere banco: Telecom investirà tre milioni di euro per lo sviluppo della banda larga. Ad annunciarlo è l'amministratore delegato Franco Bernabè intervistato da Lucia Annunziata, che difende il suo operato alla guida del colosso delle telecomunicazioni tentando di evitare lo scorporo delle rete di Telecom Italia

ipotizzato dal CDA per tentare di salvare l'azienda. Telecom mette sul piatto tre miliardi che però, ad oggi, non ci sono: gli azionisti dovrebbero rinunciare a parte dei dividendi per poter recuperare questi fondi e finanziare lo sviluppo del progetto. In ogni caso, considerato lo stato delle infrastrutture di rete che abbiamo, tre milioni di euro (peraltro stanziati in tre anni) potenzierebbero poco o nulla. Staremo a vedere.

Fra realtà aumentata, subvertising, steampunk e performance retrospettiva dal 2° raduno artivista made in Italy

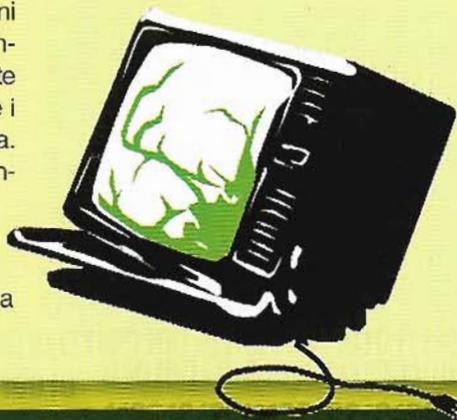
AHAcktitude 2009

Il 27, 28 e 29 novembre a Milano presso il CS Cantiere si è svolto AHAcktitude 09, il 2° raduno organizzato dagli iscritti di AHA, la lista italiana che dal 2002 mantiene vivo il dibattito su activism, hacking e artivism. Come sempre HJ c'era ed eccoci qua con una retrospettiva su un evento che merita la nostra attenzione.

:: About

AHAcktitude si ispira al modello HackMeeting. Il primo incontro embrionale è avvenuto nel novembre 2008 presso il SALE di Venezia. Ma quest'anno sono molte le novità a partire dal nome. In un fresco gioco di parole, AHAcktitude unisce la sigla della lista al concetto di attitudine: una scelta efficace per un evento che intende collocarsi in quella zona dove l'arte si incontra con l'attivismo sociale e tecnologico nel tentativo di aprire un dialogo e condividere pratiche, concetti, azioni con i movimenti di base. Fra seminari, workshop, presentazioni e performance, una densa tre giorni di attività declinata all'insegna dell'opensource, indagando le problematiche legate ai social network, il cyberpunk, il fake e i nomi collettivi, fino alla realtà aumentata. Mossi da un assunto di base forte e condivisibile: "occorre costruire esperienze, perché la comunicazione senza i corpi comunica solo i messaggi preconfezionati, e il corpo senza intelligenza produce solo manipolazione".

:: Corpi e risorse

AHAcktitude è un evento "emergente". Non si basa su dinamiche economiche, commerciali e nemmeno "curatoriali" in senso stretto, ma è il frutto di una dinamica e di rapporti sociali di reciprocità e scambio e della volontà libera di individui che hanno in comune risorse (intellettuali e materiali: si pensi al tempo, ad esempio) e competenze. Senza questi legami e senza la volontà di questi individui l'evento semplicemente non avrebbe luogo, svuotato non solo di senso ma anche delle forze che lo animano. Quei corpi che discutono, pensano, agiscono fuori, dentro e in prossimità della lista. Nel panorama italiano, questi corpi coincidono con artisti che amano manipolare il codice (del software e della

Materiale grafico per spillette da autoprodurre con i loghi dell'evento.

comunicazione), studenti dell'accademia (e non solo), docenti universitari, hackers, curatori, persone che simpatizzano, appoggiano o promuovono dall'interno le esperienze e i movimenti sociali di base (senza la pretesa né di rappresentarli né di esaurirne il numero): in due parole il popolo degli artivisti. Sono le loro ricerche, le loro opere, le loro azioni e performance che hanno dato forma e sostanza al programma attraverso una modalità emergente basata sul confronto diretto. Dallo steam punk all'uso dei nomi collettivi come San Precario, Anna Adamolo o Serpica Naro; dall'analisi critica della realtà aumentata al laboratorio nomade di phisical computing dell'Accademia di Carrara; dal subvertising al green washing; dalle estetiche mobili realizzate con video cellulari alla bluetooth war per invadere i flussi comunicativi della metropoli fino all'analisi della Google-crazia, un susseguirsi di seminari, workshop e presentazioni che hanno saputo unire alla riflessione teorica l'attenzione alle pratiche e il desiderio di comprendere e trasformare attivamente la realtà. Decostruendo le visioni propagandistiche e precostituite della realtà e verità oggettive di ogni genere. Per farsi un'idea precisa del programma consigliamo inoltre di curiosare sul sito del Cantiere che raccoglie un'ottima selezione di video ripresi e montati durante l'evento.

AHACKTITUDE '09

www.ahacktitude.org/event

27 28 29 NOVEMBRE MILANO CS CANTIERE

All'indirizzo www.cantiere.org troviamo riprese video e fotogallery di tutti gli interventi dell'evento.

:: Alchimie generazionali

Concludiamo questa retrospettiva con una riflessione sui corpi e sull'artivismo. Si è realizzata una particolare alchimia in questo AHAcktitude, anche grazie al lavoro di connessione e di presenza con il Cantiere e con il collettivo Aut Art nato nelle aule occupate dell'Accademia di Brera, che ha permesso di aprire un interessante link "generazionale" fra realtà artistiche-attiviste focalizzate sull'uso, comprensione e decostruzione di tecnologie e media digitali e quei giovanissimi che dalle università hanno sollevato l'Onda Anomala in Italia l'anno scorso: diverse coincidenze hanno inoltre cospirato affinché proprio da AHAcktitude venerdì 28 ci fosse un collegamento in diretta con gli studenti che in questo momento stanno occupando oltre 30 atenei in tutta la Germania, passando per l'Austria e la Svizzera. Il tutto via Skype da un aula magna di Monaco e nel più semplice dei modi (una webcam e una connessione Internet), ma con un effetto potentissimo per i presenti a dimostrare un assunto di base: l'innovazione è sociale e culturale prima ancora che tecnologica, e trova il suo senso se incorporata, appropriata e agìta all'interno di tali processi. A modo loro questi "nuovi" (più o meno giovani) hanno molto da comunicare e comunicarsi. Proprio a partire dai linguaggi, dal bisogno/diffusione di pratiche, dal raccontarsi storie probabilmente vicine e affini. Speriamo che lo facciano e che eventi come AHAcktitude possano farsene tramite.

INCONTRO ALL'INTERNO DEL CICLO DI AUTOFORMAZIONE "INDUSTRIA CREATIVA E OPEN SOURCE" ORGANIZZATO DA AUTART

WARM UP AHACKTITUDE 2009

OPEN SOURCE

AUDIO E VIDEO STREAMING

lecture: teoria e pratica dello streaming

Durante questo seminario verrà analizzata la tecnica dello streaming tenendo presente le origini di tale sviluppo e gli strumenti tecnici necessari, mentre una breve panoramica della storia della trasmissione del segnale audio e video (radio, televisone, internet) e dei supporti (video cassette a nastro, dischi, cd, dvd, hard disks) verrà delineata sullo sfondo. Particolare attenzione verrà data alle nuove possibilità che l'open publishing, ovvero la possi-

25 ORE 9:30 AULA 210

NOVEMBRE

26 ORE 12:30 AULA 210

Warm up organizzato all'Accademia di Brera nel programma di autoformazione studentesca.

penelope.di.pixel

Stop al canone RAI

Come e quando non pagarlo

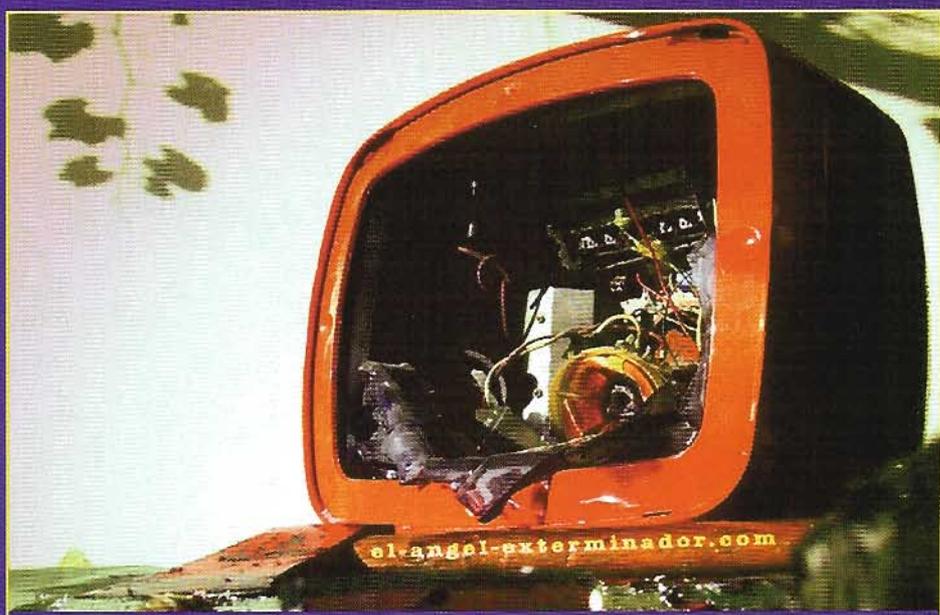
La fine dell'anno porta con sé numerosi avvenimenti: il Natale, il capodanno e... il pagamento del canone RAI. Quest'ultimo, la cui ricorrenza non è forse la più apprezzata fra le varie del mese di Dicembre, sembra per molti essere una sorta di male necessario, per altri un furto legalizzato, per altri ancora un pizzo che dev'essere evitato in qualsiasi modo. A prescindere dalla qualità dei programmi trasmessi in TV e dall'opportunità o meno di pagare per vederli, il problema principale è la poca chiarezza della normativa, insieme a una serie di pratiche non propriamente cristalline degli incaricati RAI, che spesso portano a far pagare questa imposta anche persone che di diritto potrebbero evitarlo.

:: Cos'è il canone RAI

Il canone RAI è un'imposta sul possesso di apparecchi riceventi trasmissioni radiotelevisive. Innanzitutto, in quanto imposta, esso si distingue dalla tassa perché il suo pagamento non è collegato a una specifica prestazione da parte dello Stato. Detto in soldoni: non importa quanto ci faccia schifo Domenica In, noi dobbiamo pagare per il solo fatto di possedere un televisore. Anzi, la situazione è molto peggiore: è necessario pagare anche se il televisore è configurato per non ricevere la RAI, anche se il segnale RAI non arriva al nostro edificio e anche se il televisore non è collegato a un'antenna o a una presa di corrente! Il canone è, in un certo senso, ereditario, nel senso che come passa di mano una TV così deve fare il relativo abbonamento; addirittura, in caso di decesso di un abbonato RAI l'erede deve richiedere l'intestazione dell'abbonamento a proprio nome.

:: Chi deve pagare?

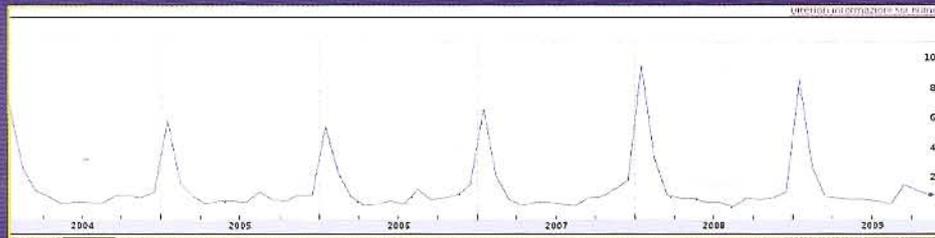
Il soggetto tenuto a pagare il canone RAI è il detentore dell'apparecchio radiotelevisivo, quindi non importa se la TV è di proprietà, in prestito o in affitto. L'abbonamento copre tutti gli apparecchi detenuti presso la propria residenza o presso la propria dimora abituale e secondaria, quindi non è necessario pagare un canone per ogni abitazione si abbia

a disposizione. Dal 1997 non è più obbligatorio pagare per il possesso di un'autoradio, e dal 2008 sono esenti i soggetti di età pari o superiore ai 75 anni, con un reddito complessivo (proprio e del coniuge) non superiore a 516,46 euro al mese. Ma attenzione, in questo caso specifico l'esenzione vale solo per l'apparecchio che si trova nel luogo di residenza. Il vero problema, tuttavia, è la definizione di "apparecchio radiotelevisivo": rifacendosi a un regio decreto risalente al 1938 (tempo in cui i lungimiranti legislatori avevano sicuramente previsto la comparsa di PC in ogni casa, Internet e videofonini), viene definito come tale ogni apparecchio atto o adattabile alla ricezione delle trasmissioni radiotelevisive. All'indirizzo http://bit.ly/8wh14c è descritta un'indagine dell'ADUC (Associazione per i Diritti degli Utenti e Consumatori) fatta interpellando gli operatori del call center RAI, da cui sono emerse definizioni varie e contraddittorie che comprendevano, fra gli apparecchi radiotelevisivi, videocitofoni, modem e fotocamere digitali. All'atto pratico, se abbiamo un classico televisore c'è poco da fare: siamo tenuti per legge a pagare il canone. Se, invece, disponiamo di altri tipi di apparecchi che non sappiamo se classificare come radiotelevisivi, possiamo inviare un interpello all'Agenzia delle Entrate (inviando a mezzo raccomandata il modulo all'indirizzo http://bit.ly/6LnDJV). In caso di mancata risposta, o qualora gli apparecchi non siano da considerare come televisori, saremo legittimati a non pagare il canone fino a che non ci verrà comunicato diversamente dall'Agenzia stessa. Infine, se siamo abbonati RAI possiamo effettuare una disdetta: è sufficiente mandare una raccomandata indicando il numero di abbonamento e specificando a chi si desidera cedere l'apparecchio, oppure richiedendo di suggellare il televisore. In questo caso l'utente si impegna formalmente a non utilizzare più la propria TV (un tempo "suggellata" all'interno di un sacco di juta, operazione che ora avviene solamente di rado): una descrizione dettagliata della procedura è presente all'indirizzo http://www.beppegrillo.it/iniziative/cancelliamoilcanone/.

Non importa se la vostra TV è vecchia, brutta o addirittura non funziona: il solo fatto di osare tenerla in casa vi rende passibili di imposta RAI!

:: Come non pagare

Anche quando siamo dalla parte della ragione risulta comunque molto difficile non pagare il canone: è sufficiente cambiare residenza, infatti, per cominciare a ricevere al nuovo indirizzo una serie di missive, sempre più minacciose, che richiedono l'attivazione immediata di un abbonamento, al punto da richiedere una comunicazione ad hoc del Garante della Privacy. Le associazioni per la tutela dei consumatori ricevono migliaia di segnalazioni in cui vengono descritti i metodi intimidatori (e non sempre legittimi) che la RAI usa per far pagare il canone praticamente a chiunque: all'indirizzo http://www.damiduck.it/rai.htm, ad esempio, è possibile leggere il resoconto di un tentativo di suggellamento durato addirittura diversi anni. Per difenderci da queste vere e proprie aggressioni possiamo consultare il vademecum pubblicato su http://bit.ly/7hqWAY, che consiglia il comportamento da tenere in diverse occasioni, dalla visita a domicilio di un funzionario RAI (che, per inciso, non ha alcun diritto di entrare in casa di un privato cittadino) alla richiesta di dichiarazione sostitutiva dell'atto di notorietà.

:: Conclusioni

I programmi di qualità presenti alla TV si contano sulle punte delle dita; tuttavia, a meno che non decidiamo di rinunciare completamente al possesso di un televisore, è bene ricordare che siamo ugualmente tenuti per legge a pagare il canone RAI. Se invece scegliamo di vivere senza TV, oppure se disponiamo di apparecchi che non sappiamo se classificare come radiotelevisivi, è utile sapere che, nonostante le prepotenti richieste della RAI, non siamo tenuti a pagare il canone e che ci sono informazioni e strumenti a disposizione per far valere i nostri diritti.

Stando a quanto ci dice Google insights, chi l'avrebbe mai detto, l'interesse verso il canone RAI ha dei picchi annuali vic ini alla scadenza del pagamento.

Il sistema operativo gestisce la memoria di un'applicazione attraverso complesse strutture

Il lato oscuro della memoria

Quando scriviamo e compiliamo un programma le cose non sono semplici come sembra. Gcc (il nostro fido compilatore della gnu) fa sembrare le cose facili: scriviamo sulla riga di comando "gcc -o nome nomesource.c" premiamo invio e il nostro programma è pronto per l' uso. Ma come è costruita all' interno la nostra applicazione? com'è suddivisa? Al proprio interno il nostro file viene diviso in contenitori, ognuno dei quali con un proprio compito, che darà la possibilità di organizzare tutte le variabili nella memoria. Nel caso dei file elf (executable and linkable format), gli eseguibili in sistemi unix-like, una delle parti più importanti è il "Program Header", un contenitore che descrive e definisce le informazioni essenziali del programma, come l' architettura della macchina su cui può essere eseguito, l' indirizzo di memoria della prima istruzione ("Entry Point") e gli indirizzi per accedere agli altri contenitori (o sezioni). Il compito invece di analizzare ogni sezione viene assegnato al "Section Header", una struttura (presente nell' header /usr/include/elf.h insieme al "Program Header") che definisce un' unica tipologia di informazioni, come codice sorgente, variabili o simboli. Ad ogni sezione può essere riferito uno o più segmenti che a differenza delle ultime, descrivono in che modo il contenuto delle sezioni deve essere caricato in memoria e quali caratteristiche deve avere. I segmenti più importanti sono quelli che andremo a trattare in questo articolo e sono i segmenti testo, dati e bss, a cui si aggiungono lo heap e lo stack, importantissimi per l' organizzazione di variabili dinamiche e locali.

:: Il Segmento testo

Il segmento di testo (o codice) è proprio quella parte che contiene il codice del nostro programma, (certamente una volta compilato, quindi in assembly). La sua memoria è fissa, non cambia, per-

```
typedef struct
{
  unsigned char e_ident[EI_NIDENT];     /* Magic number and other info */
  Elf32_Half    e_type;                 /* Object file type */
  Elf32_Half    e_machine;              /* Architecture */
  Elf32_Word    e_version;              /* Object file version */
  Elf32_Addr    e_entry;                /* Entry point virtual address */
  Elf32_Off     e_phoff;                /* Program header table file offset */
  Elf32_Off     e_shoff;                /* Section header table file offset */
  Elf32_Word    e_flags;                /* Processor-specific flags */
  Elf32_Half    e_ehsize;               /* ELF header size in bytes */
  Elf32_Half    e_phentsize;            /* Program header table entry size */
  Elf32_Half    e_phnum;                /* Program header table entry count */
  Elf32_Half    e_shentsize;            /* Section header table entry size */
  Elf32_Half    e_shnum;                /* Section header table entry count */
  Elf32_Half    e_shstrndx;             /* Section header string table index */
} Elf32_Ehdr;

dir31@Dir31-GetMe:~$ import Ehdr.jpg
```

Struttura del program header definita in usr/include/elf.h.

```
typedef struct
{
  Elf32_Word    sh_name;                /* Section name (string tbl index) */
  Elf32_Word    sh_type;                /* Section type */
  Elf32_Word    sh_flags;               /* Section flags */
  Elf32_Addr    sh_addr;                /* Section virtual addr at execution */
  Elf32_Off     sh_offset;              /* Section file offset */
  Elf32_Word    sh_size;                /* Section size in bytes */
  Elf32_Word    sh_link;                /* Link to another section */
  Elf32_Word    sh_info;                /* Additional section information */
  Elf32_Word    sh_addralign;           /* Section alignment */
  Elf32_Word    sh_entsize;             /* Entry size if section holds table */
} Elf32_Shdr;

dir31@Dir31-GetMe:~$ import Shdr.jpg
i love pixie
```

Struttura del section header definita in usr/include/elf.h.

```
#include <stdio.h>

int global_var;

void esempio()
{
 int stack;
 printf("(stack) Indirizzo della variabile stack: 0x%x\n\n",&stack);
}
main()
{
 static int i=2;
 char *b= (char*)malloc(20);
 strncpy(b,"ciao hacker journal\n",20);

 printf("\n(data segment)Variabile statica inizializzata: 0x%x\n\n",&i);
 printf("(bss) Variabile globale non inizializzata: 0x%x\n\n", &global_var);
 printf("(heap)Puntatore b (allocazione della memoria): 0x%x\n",&b);
 printf("      Il suo valore: %s\n\n",b);
 esempio();
}

dir31@Dir31-GetMe:~/hacker journal$ import esempio.jpg
```

Codice sorgente del nostro esempio.

```
dir31@Dir31-GetMe:~/hacker journal$ ./esempio

(data segment)Variabile statica inizializzata: 0x804976c

(bss) Variabile globale non inizializzata: 0x8049774

(heap)Puntatore b (allocazione della memoria): 0xbf9dd800
      Il suo valore: ciao hacker journal


(stack) Indirizzo della variabile stack: 0xbf9dd7d4

dir31@Dir31-GetMe:~/hacker journal$ import esempio.jpg
```

Ecco che la nostra applicazione viene eseguita, a voi il compito di darla in pasto ad un debugger.

chè non deve contenere variabili.Le sue istruzioni vengono eseguite una alla volta, ma non in modo lineare, in quanto esistono strutture, classi, metodi, funzioni, ecc..., che portano a far eseguire parti di codice magari scritte molto più avanti o molto prima nel listato del sorgente. Il compito di tenere l' ordine di ogni istruzione viene affidato ad un puntatore: l' "EIP". Una volta eseguito, il programma stringe un rapporto molto stretto con questo puntatore, leggendo l' istruzione puntata dall' EIP e aggiungendo ad esso la lunghezza in byte dell' istruzione letta ed eseguendola. Tutto questo in modo ciclico finchè non si arriva ad una chiusura normale o anomala dell' applicazione. Il segmento di testo inoltre non ha permesso di scrittura, poichè è bene evitare qualsiasi tentativo di modifica del codice.

:: Il segmento dati e Bss

Il segmento dati (data segment) contiene le variabili statiche e globali inizializzate del programma, mentre il segmento bss contiene le stesse non inizializzate. Anche questi segmenti hanno una memoria fissa, perchè vivono durante l' esecuzione del programma memorizzate in loro segmenti di memoria. Il permesso di scrittura però è abilitato.

:: Heap

Il segmento heap è una parte molto particolare della memoria che il programmatore può toccare con mano. È un segmento dinamico che si gonfia e si restringe a seconda delle necessità. Viene gestito dal programmatore attraverso le funzioni di allocazione dinamica della memoria e dal processore attraverso complessi algoritmi. Lo heap si espande poi, sempre verso indirizzi di memoria più alti, accostandosi allo stack.

:: Stack

Quest' ultimo è un segmento altrettanto particolare e molto analizzato soprattutto in fase di bug-hunting ed exploiting. Viene utilizzato come contenitore temporaneo di variabili e dati nelle chiamate a funzione, anch' esso di dimensione variabile. Quando infatti l' EIP arriva ad una chiamata a funzione (jump, call, branch, ecc..) ci saranno sicuramente delle variabili che verranno passate come argomento. Lo stack ci arriva in aiuto prendendo in consegna queste variabili (compreso l' indirizzo di ritorno all' istruzione del programma che servirà per riportare l' EIP all' indirizzo corretto una volta terminata la procedura) e conservandocele per gli utilizzi all' interno della fuzione stessa. Lo stack ha una struttura FILO (first in – last out), quindi il primo elemento ad entrare sarà l' ultimo ad uscire, proprio come se fosse un filo con un nodo all' estremità a cui vengono aggiunte delle perline. Per tenere traccia dei dati nello stack si utilizza un registro: l' ESP. Questo è un puntatore alla cima dello stack quindi tiene conto degli elementi presenti partendo da quello inserito per ultimo. I dati in questo segmento si inseriscono attraverso l' istruzione assembly "push" e vengono estratti tramite l' istruzione "pop", facendolo espandere verso indirizzi più bassi verso lo heap.

:: Esempio

Consideriamo ora un esempio di codice, lo troviamo nella sezione Codice su hackerjournal.it.

Il codice presentato è un banalissimo programmino in C, che contiene diversi tipi di variabili: una variabile globale non inizializzata in testa al codice, una variabile in una funzione, una static inizializzata e un puntatore a cui abbiamo allocato 20 byte di memoria. Vediamo come si comportano: una volta che il programma viene eseguito, il codice compilato viene inserito nel segmento di testo, mentre ogni variabile verrà ordinata nel proprio segmento di competenza in base alla propria definizione. Gli indirizzi di memoria più bassi individuano il segmento di testo, cui segue il segmento dati, bss, heap e stack che è rappresentato da indirizzi di memoria più alti. Nel data segment verranno organizzate tutte quelle variabili statiche e globali inizializzate, e in questo caso quindi il segmento conterrà la variabile statica definita nella main. Nel bss invece sarannò destinate le controparti del data segment, quindi le variabili non inizializzate come quella globale in cima al codice. Successivamente si arriva nello heap. In questo segmento verrà indirizzata la variabile "b", a cui sono stati allocati 20 byte di memoria. Lo heap infatti viene caricato con questa porzione di memoria e si espande verso l' alto per fare posto alla dimensione della variabile. Infine si arriva allo stack che in questo caso non ha nessuna variabile di argomento da contenere e deve solo calcolare i byte da riservare per le variabili locali e salvare l' indirizzo di ritorno. Una volta fatto questo creerà quindi un frame (un pacchetto) e vi inserirà questi dati (processo noto come "prologo della funzione"). A questo punto la funzione verrà eseguita normalmente e alla sua conclusione, prima di eliminare il frame, l' esecuzione del programma passera di nuovo alla funzione main().

Dir31

EDC: LA TERZA STRADA

C'è un modo nuovo di fare economia che sa molto di cultura Hacker con la H maiuscola

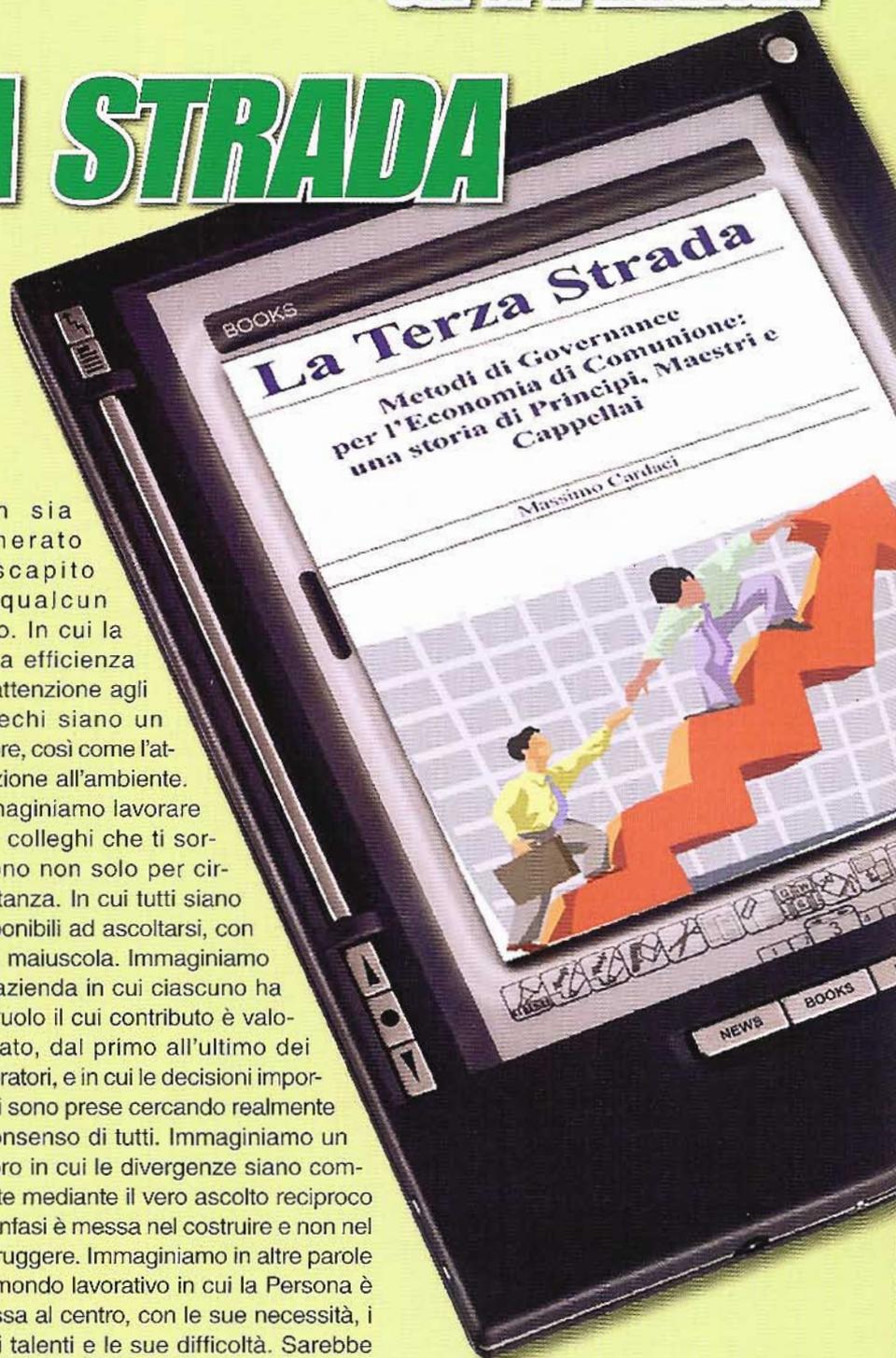
La Terza Strada
Metodi di Governance per l'Economia di Comunione: una storia di Principi, Maestri e Cappellai
Massimo Cardaci

Crisi economica, lavoro difficile da trovare o mantenere, finanza che gioca a fare la creativa. E noi in mezzo (qualcuno direbbe "e io pago..."). Si può subire passivamente o provare a capire, per vedere se possiamo fare qualcosa. A noi piace capire.

:: Capitalismo e socialismo pari sono

Economisti e politici penseranno "che sciocchezza", passando avanti (ma noi siamo gente curiosa e continuiamo a leggere: almeno è un messaggio nuovo). Entrambi i sistemi si basano infatti su un elemento comune: mettere al centro il capitale. Uno per divinizzarlo, l'altro per demonizzarlo. E c'è altro: entrambi hanno dimostrato di essere inadeguati a supportare un sistema di crescita sostenibile. Sembrerà una semplificazione eccessiva, ma spesso è proprio dall'estrarre gli elementi importanti che si ricavano le soluzioni migliori, quelle che non si perdono in dettagli inutili.

:: Immaginare un'utopia

Immaginiamo quanto sarebbe bello lavorare in un ambiente in cui ci si aiuta e la conoscenza di ciascuno è un bene che viene volentieri condiviso con gli altri. In cui il profitto prodotto col proprio lavoro non sia generato a scapito di qualcun altro. In cui la sana efficienza e l'attenzione agli sprechi siano un valore, così come l'attenzione all'ambiente. Immaginiamo lavorare con colleghi che ti sorridono non solo per circostanza. In cui tutti siano disponibili ad ascoltarsi, con la A maiuscola. Immaginiamo un azienda in cui ciascuno ha un ruolo il cui contributo è valorizzato, dal primo all'ultimo dei lavoratori, e in cui le decisioni importanti sono prese cercando realmente il consenso di tutti. Immaginiamo un lavoro in cui le divergenze siano composte mediante il vero ascolto reciproco e l'enfasi è messa nel costruire e non nel distruggere. Immaginiamo in altre parole un mondo lavorativo in cui la Persona è messa al centro, con le sue necessità, i suoi talenti e le sue difficoltà. Sarebbe proprio un bel mondo.

:: EdC, chi è costei?

Era il 1991, in Brasile, quando fu proposto un modo diverso di fare Economia. Idea tanto semplice quanto innovativa: mettere al centro dell'agire economico un soggetto diverso, che non sia il capitale ma la persona. Idea audace, perché comunque non si trattava di creare una nuova ONLUS (Organizzazione senza fini di lucro) o una Cooperativa, ma piuttosto di creare un modo di fare Azienda, e quindi di generare profitto, che fosse sostenibile.

Le regole sono semplici, sulla carta.

Il modello di gestione deve garantire di mettere la Persona al centro, e non il capitale. Questo deve essere supportato da un rinnovamento della cultura aziendale che ponga la "cultura del dare" come fondamento dell'agire economico interno ed esterno (cioè anche verso utenti e fornitori, anche quelli più rom... scatole). Già queste sono regole forti da mettere in pratica, eppure non è tutto. Infatti è anche stabilito che gli utili siano gestiti in un modo particolare.

Un terzo deve essere reinvestito per la crescita dell'Azienda, intesa come infrastrutture e (non "o") persone che vi lavorano. Un altro terzo va utilizzato per migliorare la condizione degli indigenti della zona in cui l'azienda opera ovvero migliorare la loro condizione in modo strutturale e non solo assistenzialistica. Ad esempio formandoli ed assumendoli, o finanziando attività che li possano rendere economicamente autosufficienti, diventando a loro volta parte attiva del "progetto". Infine un ultimo terzo deve essere utilizzato per supportare la formazione di coloro che vogliono apprendere questo nuovo modo di fare azienda e di vedere l'economia.

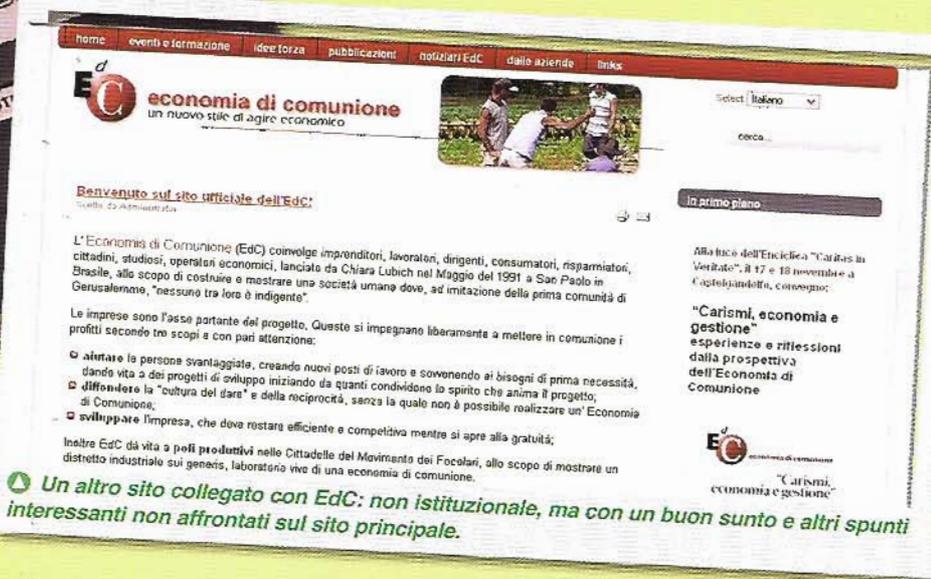
Il nome che gli fu dato è "Economia di Comunione" (niente a che fare con Comunione e Liberazione).

Il sito istituzionale dell'Economia di Comunione, dove approfondire il tema. Qui possiamo trovare tantissimo interessante materiale.

:: Una utopia?

Le regole sono forti, difficili da assimilare, e non ammettono "mezze misure": o si fa bene, o non serve a nulla. Eppure oggi ci sono nel mondo 800 Aziende che operano secondo il modello EdC, dal Brasile agli USA, dalla ex Yugoslavia alle Filippine, dalla Francia all'Italia. E ci sono anche 7 poli industriali.

Entrando in queste aziende si tocca con mano quel mondo che abbiamo descritto "una possibile utopia". Gente che lavora sodo e che lo stipendio se lo suda, ma nei cui occhi brilla una luce diversa e le cui mani sono pronte a fermarsi per ascoltare (con la A maiuscola) chi gli si rivolge. In più, le numerosissime tesi e studi provenienti da ogni angolo della terra hanno portato gli Economisti ad inserire nel loro vocabolario e nei processi finanziari, termini come "gratuità", "felicità", "beni relazionali" e tante altre cose che fino a poco tempo fa si ritenevano solo parte della sociologia. Qualche anno fa sarebbe stato impensabile considerare questi elementi come "intangibili" e trattarli nella pianificazione economica e nell'accounting finanziario come dei veri e propri "asset".

Ovvero, il profitto non è più distinto dalla persona che lo genera e dal motivo per cui lo genera. Per anni gli economisti hanno detto che un'Azienda EdC non sarebbe potuta sopravvivere nel mercato, eppure queste aziende continuano ad esistere, ad aumentare di numero e, cosa non trascurabile, a generare profitto.

Un altro sito collegato con EdC: non istituzionale, ma con un buon sunto e altri spunti interessanti non affrontati sul sito principale.

Port knocking in ambito locale e remoto in C

Knock... Knock... MAC e URL Wrappers!

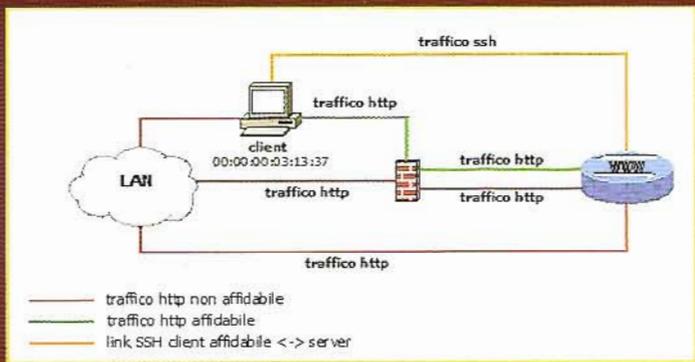
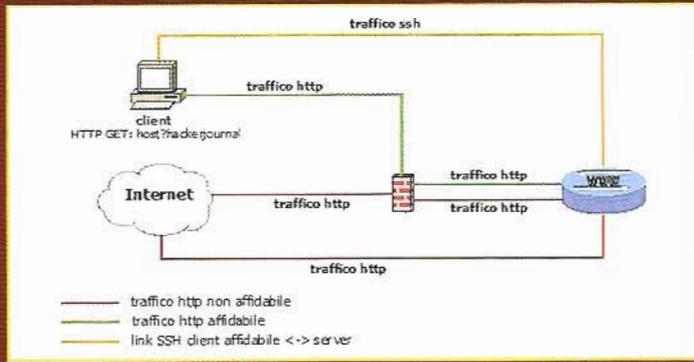
Prima di addentrarci nella trattazione è necessario chiarire cosa significhi il termine "port knocking" in ambito di reti informatiche e quali siano i benefici fruibili da questa tecnica. In linea generale il termine "port knocking" descrive una metodologia attraverso la quale è possibile accedere a un servizio ospitato su un server senza che questo sia effettivamente attivo. Esistono numerose e distinte implementazioni in tal senso, alcune di queste si basano sull'invio di particolari pacchetti a porte chiuse e controllate da un packet filter; quando questi sono ricevuti dal server vengono analizzati ed associati a determinate azioni che quest'ultimo intraprenderà. Non ci prolunghiamo ulteriormente nella trattazione dei vari modi di intendere il "port knocking" ed offriamo di seguito una panoramica, quanto più ampia possibile, di quello che andremo a realizzare. Il codice integrale lo troviamo sul sito di hackerjournal.it nella sezione Codice.

:: Portknocking in ambito locale

Proiettiamoci in una situazione tipica all'interno una rete LAN: un server web per l'accesso INTRANET al quale fanno riferimento i vari client (si pensi ad un'azienda di piccole e medie dimensioni). Domandiamoci ora se, in qualche modo, sia possibile abilitare il servizio SSH solo quando necessario. Se sì, come potremmo far si che sia uno ed un solo client a poter richiedere l'attivazione dello stesso? A tal riguardo possiamo pensare di implementare uno script che avvii il servizio SSH solo quando a richiederlo è un particolare MAC address associato al client "certificato" della nostra LAN. Avendo supposto la presenza di un webserver attivo ospitato sul server ed in riferimento a quanto ipotizzato prima, diviene fondamentale realizzare un semplice MAC wrapper che intercetti tutte le richieste HTTP indirizzate al server ricercando quella che contenga il MAC Address autorizzato; se questa ricerca offrirà risultati positivi allora lo script si occuperà dell'inizializzazione del demone SSH. Procediamo dunque con la realizzazione dello script da avviare sul server, facendo conto che il MAC Address relativo al client considerato affidabile sia 00:00:00:03:13:37.

1. In prima istanza utilizzeremo le librerie libpcap ed ethernet per sniffare tutti i pacchetti di tipo http e controllare i MAC Address.

2. Ci occuperemo quindi di scrivere una funzione che analizza tutti i MAC Address alla ricerca di quello autorizzato; qualora vi siano riscontri avvieremo il servizio SSH.

3. Definiamo, dunque, una funzione di loopback che estragga il MAC Address da ogni pacchetto intercettato, per ognuno di questi utilizzeremo la funzione precedentemente realizzata alla ricerca di quello autorizzato. Infine, imposteremo un filtro per la cattura dei soli pacchetti TCP destinati alla porta 80 ed avvieremo lo sniffer: Realizzato lo script, assicuriamoci che sul server sia attivo esclusivamente il web

La rappresentazione schematizzata del processo di abilitazione del servizio SSH effettuato dal nostro script.

Lo schema del processo di abilitazione del servizio SSH da remoto effettuato dal nostro script.

server e testiamo il lavoro svolto.

4. Una volta compilato, avviamo il MAC Wrapper.

5. Dal client autorizzato proviamo ad inviare una richiesta HTTP al web server; prima di farlo, però, ci preoccuperemo, ovviamente, di modificare il MAC Address dell'interfaccia di rete.

6. Fatto questo, controlliamo se effettivamente il servizio SSH è stato avviato dal server.

:: Portknocking in ambito remoto

Occupiamoci ora di realizzare uno script che ci consenta di avviare il servizio SSH anche da remoto. Lo scenario tipico d'utilizzo potrebbe essere un server web sul quale vogliamo attivare il login remoto solo quando necessario riducendo al minimo il rischio di attacchi dovuti alla presenza di un servizio sempre attivo. A titolo esemplificativo, realizzeremo uno script che avvii il demone SSH solo quando sia inviata una ben determinata stringa al server web in questione (considereremo, pertanto, questa stringa una sorta di passkey di abilitazione al servizio SSH). Il nostro environment è composto da un web server apache ospitato sul sistema operativo GNU/Linux Debian dal server remoto. Un'opportuna riflessione ci suggerisce che un modo per analizzare gli indirizzi in questo contesto è dato dai log di accesso di apache. Dovremo quindi realizzare una copia dei log di apache avendo cura di eliminare gli eventuali riferimenti alla password già presenti e restare in ascolto analizzando tutte le richieste destinate al web server. Quando sarà formulata una richiesta di tipo hostname?password allora faremo sì che il servizio SSH prenda vita. I log di accesso di apache su Debian sono generalmente memorizzati nella cartella /var/log/apache/access.log; creeremo pertanto un loop che si occupi di copiarli, eliminare le eventuali occorrenze alla password già presenti e iniziare a ricercare la password definita.

7. Per farlo, prima di tutto, definiamo il percorso dei log e la password che attiverà SSH.

Realizziamo quindi il parser che si occuperà della ricerca della stringa verificando, per ogni riga del log, se la password corrisponde effettivamente a quella definita ed in caso affermativo effettuiamo la copia del file di log di Apache eliminando le occorrenze trovate:

8. Avviamo, in questo caso, SSH e ripristiniamo i log di apache. Se la ricerca non offrirà riscontri, invece, eseguiremo semplicemente un'istruzione nulla e rimarremo in ascolto.

9. Per aprire il file di log di apache e leggerlo utilizzeremo un semplice ciclo che punti alla funzione check_logs() appena realizzata.

10. Anche in questo caso verifichiamo il lavoro svolto utilizzando il nostro strumento preferito: il terminale.

11. Avviamo l'URL wrapper sul server remoto.

12. Da remoto, quindi, inviamo una richiesta al server utilizzando la passkey definita.

13. Controlliamo ora se sul server abbiamo ottenuto l'effetto desiderato.

:: Conclusioni:

Che il nostro fine ultimo sia la realizzazione di un'infrastruttura di rete estremamente sicura o la programmazione di una sofisticata backdoor che si attivi solo a determinate sollecitazioni, sicuramente il lettore avrà, a questo punto, intuito che esistono innumerevoli implementazioni di port knocking realizzabili che hanno come unico ostacolo esclusivamente la fantasia. Vi esortiamo quindi a realizzare la vostra, magari prendendo spunto da quanto appreso in questo articolo.

Giovanni Federico

Scaricare un file con eMule richiede mesi? Con il client giusto si riducono i tempi, però...

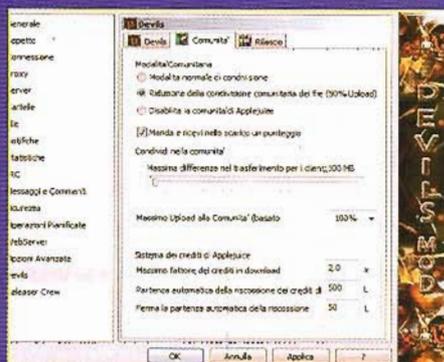
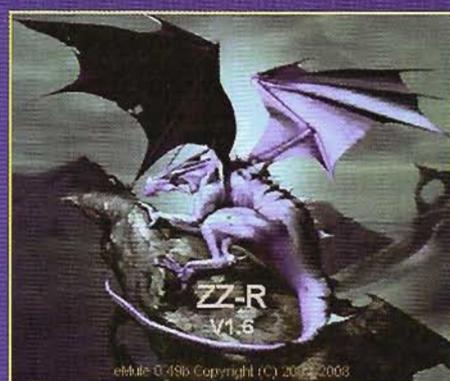
Vampiri della condivisione

Tutti conosciamo eMule, è uno tra i programmi per il P2P più utilizzati in Italia e sicuramente il più famoso, anche se spesso fama e qualità non vanno di pari passo. Chi ha provato a utilizzarlo almeno una volta (e soprattutto lo utilizza sporadicamente) sa di cosa stiamo parlando: ha un ottimo bacino di fonti e consente di trovare anche file considerati rari, ma tra il clic per avviare il download e lo start effettivo ci passano le calende greche, sempre che nel frattempo non abbiamo deciso di annullare l'operazione cercando il contenuto che ci interessa con altri sistemi. Tanti file, tante fonti ma tempi lunghi... perché? Il sistema adottato dal Mulo per gestire l'accesso al download di un file è basato sullo scambio di crediti. Quando qualcuno scarica un file utilizzando materiale che abbiamo messo in condivisione acquisiamo uno (o più, a seconda della modalità che abbiamo scelto) crediti, quando proviamo a downloadare un file che ci interessa ci troviamo davanti alla fila di tutti quegli utenti che vogliono lo stesso file che vogliamo noi. In realtà, senza addentrarci troppo in profondità nel sistema di file transfer utilizzato da eMule, noi (e gli altri client) non scarichiamo un intero file da un'unica fonte e non siamo accodati a un unico client per scaricare il medesimo file. Ogni contenuto scambiato sulle reti eDonkey2000 (eD2K) e Kademlia viene spezzettato in tronconi da 9,28MB chiamati part, che possiamo scaricare da uno o da più client contemporaneamente. Per semplicità però, immaginiamo di scaricare da una fonte sola: noi quindi clic-

eMule ASF, un leech Mod aggressivo, che caricava i server e riempiva di spam. Ora è morto, le difese del Mulo lo hanno bannato.

chiamo sul download e ci ritroviamo all'ultimo posto della hit-parade dei downloader, indipendentemente dalla quantità di crediti maturati. La nostra fonte, ogni mezz'ora circa, dà un'occhiata alla coda di attesa e riordina la fila sulla base dei crediti che ogni client ha maturato. Chi ne ha di più ha la precedenza e a parità di crediti viene prima chi prima ha fatto la richiesta, sulla base del vecchio adagio "Chi prima arriva meglio alloggia". Va da se che se siamo dei novellini di eMule, oppure se lo abbiamo installato ex-novo e abbiamo pochi file a disposizione per l'upload o pochi client hanno scaricato utilizzandoci come fonte, noi non scaricheremo mai. Beh... proprio mai no, ma ci vorranno giorni, per non dire settimane, prima di riuscire a completare un download. Che fare? Abbandoniamo il tentativo o cerchiamo una scorciatoia? E che scorciatoia soprattutto? Una ci sarebbe, ma va contro ai principi e alla salute del file sharing e delle sue reti.

:: I vampiri

Affondano i denti nel collo delle loro vittime e ne succhiano il sangue sino a portarle alla morte, il mito di Nosferatu lo conosciamo tutti. Ora i vampiri attaccano il Mulo, si chiamano leech Mod (Mod sanguisuga), e sono client modificati (Mod appunto) da utenti stanchi di aspettare settimane per scaricare un file. Va da se che, da buoni vampiri, succhiano (in questo caso le code di attesa) e scombinano il sistema degli accodamenti e dei crediti, in quanto ingannano le fonti con crediti non loro e non mettono a disposizione file (o banda) per l'upload. È facile capire come un utilizzo massiccio di client basati su questa filosofia porterebbero in breve tempo alla morte delle reti di file sharing, con somma gioia delle Major, quindi il team di sviluppo di eMule è corso ai ripari sviluppando sistemi di difesa (i cosiddetti antileech) che bannano quei client dal comportamento scorretto o comunque deleterio per la rete. Di contro, anche chi sviluppa leech Mod non se ne sta con le mani in mano, sfornando modifiche o rilasciando nuovi client a mano a mano che quelli vecchi vengono bloccati dalle difese del Mulo. Un leecher si presenta utilizzando credenziali altrui, quindi mostrandosi come un client ufficiale e come un altro utente. Ogni utente è identificato da una stringa detta userhash, la targa che lo identifica e che serve anche per gestire le priorità di attesa in fase di download e di smistare correttamente i crediti dopo aver effettuato download e upload di part di file. Un buon vampiro, collegandosi con altri client per scaricare materiale, ha a disposizione gli userhash degli utenti con cui ha avuto a che fare e li riutilizza presentandosi sulla rete con credenziali e crediti falsi, chi ci rimette è l'ignaro utente a cui è stata rubato l'userhash, che risulterà connesso a far danni in giro per la rete anche quando non lo è. Presentandosi sotto mentite spoglie un leech Mod scala rapidamente le code di attesa, per-

DevilsMod, un client fatto per le comunità di leecher. Permetteva tempi di download ridotti per gli appartenenti alla comunità.

ZZ-R è stato uno tra i primi Bad Mod. Molto apprezzato, ha avuto aggiornamenti che gli hanno permesso una vita longeva.

mettendo download più rapidi, in più ha a disposizione una quantità infinitamente superiore di risultati alle ricerche, non avendo blocchi in tal senso. La rete eD2K è formata da client e server intermedi, che contengono le informazioni per reperire i file (nome del file ricercato e utente che lo mette in condivisione). Un client eMule normale ha a disposizione un numero limitato di risultati in ricerca, altrimenti si saturerebbero i server, un leech Mod no, quindi costringe il server a cui è collegato a una mole di lavoro che progressivamente tende a saturarlo per avere a disposizione il maggior numero possibile di file che corrispondono ai criteri di ricerca. Il vampiro è soddisfatto e il server crolla, mors tua vita mea.

:: Giochi e candele

Tempi di scarico rapidi, un bacino di materiale infinito, una scia di client derubati e di server caduti. Questo è l'operato di un leech, un client che sfrutta le falle di una rete e di un sistema diffuso come quello di eMule per ottenere il massimo con uno sforzo quasi nullo. Naturalmente la messa al bando di leech Mod avviene in tempi rapidi e in rete ce ne sono a disposizione subito di nuovi: chi scegliesse di utilizzare client del genere deve mettere in conto di dover cercare rapidamente un sostituto. Ricordiamoci che le vittime dei vampiri o diventano vampiri anch'essi (e non è questo il caso), o muoiono. Vogliamo darla vinta alle Major anche stavolta?

Cacciatori di dati

Con questo analizzatore di protocollo possiamo seguire direttamente il traffico che viaggia in una rete

Vogliamo conoscere fin nel minimo dettaglio il traffico che attraversa la nostra rete locale? Una delle migliori soluzioni è rappresentata da Wireshark (http://www.wireshark.org), un packet sniffer, o analizzatore di protocollo, open source disponibile per i sistemi operativi GNU/Linux, Microsoft Windows e Mac OS X. Scopriamo quindi come installare ed usare questa applicazione, adottando come sistema d'esempio un PC con Ubuntu 9.10 Karmic Koala inserito in una piccola LAN, tenendo presente che, installazione a parte, il suo funzionamento è sostanzialmente analogo anche nella versione per Windows.

:: Installiamo e avviamo Wireshark

Per installare Wireshark apriamo una console di terminale: entriamo nel menu Applicazioni e clicchiamo quindi su Accessori > Terminale. Nella console eseguiamo semplicemente il comando "sudo apt-get install wireshark", assicurandoci che la connessione ad Internet sia attiva. Per avviare il packet sniffer è possibile cliccare sul menu Applicazioni > Internet > Wireshark; in questo caso, però, non risulterà disponibile per l'analisi alcuna interfaccia di rete. Per utilizzarlo al pieno delle sue possibilità è necessario eseguire l'applicazione con i permessi dell'utente root: per fare questo eseguiamo in una console il comando "sudo wireshark" dove ci verrà richiesto l'inserimento della password del nostro utente principale. Wireshark presenta un'interfaccia grafica piuttosto curata. Per iniziare a catturare i pacchetti dalla rete clicchiamo sulla prima icona a sinistra nella toolbar: comparirà una finestra in cui verranno elencate le interfacce di rete disponibili, con i relativi indirizzi IP assegnati. Nella riga di ciascuna interfaccia sono presenti due pulsanti, Start e Options: il primo fa partire la cattura dei pacchetti mentre il secondo permette di impostare alcuni parametri importanti per l'operazione. Per analizzare il traffico che passa sulla

prima interfaccia ethernet, quindi, clicchiamo sul pulsante Start della riga eth0. A questo punto, nella finestra principale di Wireshark verranno mostrati i dati in transito sull'interfaccia di rete prescelta. Per terminare la cattura dei pacchetti, quindi, nella toolbar clicchiamo sulla quarta icona da sinistra, che raffigura una scheda di rete con una 'x' sopra.

:: Le informazioni fornite

Terminata la cattura dei pacchetti, cerchiamo di interpretare correttamente le molte informazioni ottenute. I dati in transito nell'interfaccia che abbiamo scelto di analizzare vengono suddivisi in righe, ciascuna delle quali è dedicata ad un singolo pacchetto. Da sinistra verso destra, quindi, ecco il significato dei campi presenti in ogni riga: innanzitutto abbiamo il numero del pacchetto (campo No.), poi a seguire il timestamp del pacchetto (Time), l'indirizzo di origine (Source) e quello di destinazione (Destination) del pacchetto, il protocollo usato (Protocol) e infine delle informazioni sul pacchetto stesso (Info). Sotto la lista dei pacchetti in transito, quindi, troviamo la sezione dell'interfaccia che mostra informazioni dettagliate sul pacchetto selezionato e, ancora più sotto, è presente una rappresentazione ASCII ed esadecimale del pacchetto stesso.

Filter: Expression... Clear Apply

No..	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.4	192.168.1.5	TCP	57937 > telnet
2	0.000096	192.168.1.5	192.168.1.4	TCP	telnet > 57937
3	0.000121	192.168.1.4	192.168.1.5	TCP	57937 > telnet
4	0.003930	192.168.1.5	192.168.1.4	TELNET	Telnet Data ...
5	0.003940	192.168.1.4	192.168.1.5	TCP	57937 > telnet
6	0.009865	192.168.1.4	192.168.1.5	TELNET	Telnet Data ...
7	0.010011	192.168.1.5	192.168.1.4	TCP	telnet > 57937
8	0.010034	192.168.1.5	192.168.1.4	TELNET	Telnet Data ...
9	0.010100	192.168.1.4	192.168.1.5	TELNET	Telnet Data ...
10	0.019228	192.168.1.5	192.168.1.4	TELNET	Telnet Data ...
11	0.021062	192.168.1.4	192.168.1.5	TELNET	Telnet Data ...
12	0.021255	192.168.1.5	192.168.1.4	TELNET	Telnet Data ...
13	0.021898	192.168.1.4	192.168.1.5	TELNET	Telnet Data ...

```
▷ Frame 1 (74 bytes on wire, 74 bytes captured)
▷ Ethernet II, Src: CompalEl_a7:8a:4e (00:0f:b0:a7:8a:4e), Dst: AsustekC_30:01:f1 (00:15:f2:30:01:f1)
▷ Internet Protocol, Src: 192.168.1.4 (192.168.1.4), Dst: 192.168.1.5 (192.168.1.5)
▷ Transmission Control Protocol, Src Port: 57937 (57937), Dst Port: telnet (23), Seq: 0, Len: 0
```

Dopo aver iniziato a catturare i pacchetti in transito su un'interfaccia, la finestra di Wireshark assumerà questo aspetto. Al centro della finestra troviamo l'elenco dei pacchetti catturati.

:: Un esempio pratico

Ora che sappiamo orientarci nei principali elementi dell'interfaccia di Wireshark, è il momento di effettuare una semplice prova di analisi. Tutti ci sconsigliano, giustamente, di usare telnet per gestire sessioni remote? A questo punto possiamo scoprire, nel modo più diretto possibile, per quale motivo una tale pratica sia fortemente sconsigliabile. Avviamo la cattura dei pacchetti sull'interfaccia eth0, quindi colleghiamoci da un PC della nostra rete locale cablata ad un altro, tramite telnet; ad esempio, dall'indirizzo IP 192.168.1.4 colleghiamoci a 192.168.1.5 lanciando il comando "telnet 192.168.1.5". Aperta la sessione telnet, inseriamo utente e password per accedere alla macchina remota, lanciamo una manciata di comandi e infine chiudiamo la sessione.

Fatto questo, torniamo alla finestra di Wireshark e terminiamo la cattura dei pacchetti. Quello che vedremo, nella lista dei pacchetti mostrata dal programma, sarà un lungo elenco di pacchetti scambiati tra gli indirizzi IP 192.168.1.4 e 192.168.1.5. Il programma mette a nostra disposizione una potente funzionalità, Follow TCP Stream, che ci permette di seguire il flusso di dati in una comunicazione TCP; tutto quello che dobbiamo fare è selezionare un pacchetto che fa parte di questo flusso: per esser sicuri, scegliamo un pacchetto con Protocol TELNET oppure con Protocol TCP e un campo Info che contenga riferimenti a telnet. Fatto ciò, premiamo il tasto destro del mouse e nel menu che appare selezioniamo la voce "Follow TCP Stream". Comparirà una finestra con la trascrizione accurata della nostra sessione telnet, compresa la password in chiaro inserita, i comandi digitati e l'output su schermo del terminale remoto! È facile immaginare, quindi, perché ovunque si sconsiglia l'uso di telnet: tutto il traffico viaggia in chiaro da una macchina all'altra, password comprese.

L'interfaccia grafica di Wireshark. A differenza di altri analizzatori di protocollo, che si utilizzano da terminale, Wireshark è dotato di un'interfaccia piuttosto curata e semplice da usare.

Io scrivo, lui spia

La verità è che non è necessario disporre di sofisticatissimi apparati come quelli che si vedono nei film per spiare ciò che viene fatto da qualcuno con il computer: basta infatti intercettare in qualche modo quanto viene scritto usando la tastiera per riuscire a ricostruire le informazioni che interessano, che siano semplici password di accesso o intere conversazioni via chat, messenger o email. Lo strumento che si usa per questa operazione di intercettazione si chiama keylogger: agisce in diversi modi e può essere più o meno sofisticato, ma il principio di funzionamento è sempre lo stesso.

:: Requisito fondamentale

Per poter installare un keylogger, qualunque sia il tipo scelto, è necessario avere accesso fisico alla macchina destinata a riceverlo, quella da tenere sott'occhio. Evitiamo volutamente di affrontare il discorso che riguarda l'installazione da remoto in quanto dovremmo in tal caso e per forza sconfinare nel campo del malware e della forzatura dei sistemi di protezione di un

Mai abbassare la guardia: ecco come funziona un keylogger e quali sono le contromisure che possiamo adottare

computer: nessuno mette in dubbio che molti malware contengano anche una funzione in grado di registrare l'input della tastiera, ma per poter spiegare tecniche simili sarebbe necessario disporre di molto più spazio. Per ora, ci focalizziamo su quei tipi di keylogger che possono essere installati potendo accedere direttamente al computer della vittima: un collega o un dipendente in ufficio, la moglie o la fidanzata che si sospetta di infedeltà e quant'altro, ognuno ha le proprie esigenze. Ricordiamoci, però, che il confine della violazione della privacy è molto sottile e saremo direttamente responsabili di quanto faremo. Hacker avvisato...

:: Tipo 1: hardware

Il primo tipo di keylogger che esaminiamo è un dispositivo hardware che va collegato al computer e che si occupa di registrare, in maniera trasparente e invisibile, quanto viene digitato sulla tastiera. I keylogger hardware possono essere caratterizzati da due tipologie costruttive. La prima, molto semplice, è costituita da un filtro che viene posto in serie al connettore PS/2 della tastiera e che registra internamente i codici dei tasti premuti. Questo keylogger deve essere periodicamente rimosso, letto con strumentazione apposita ed eventualmente reinstallato per poter proseguire nell'operazione di spionaggio. Evoluzioni di questo keylogger permettono di inviare direttamente le sequenze di codici, attraverso una connessione con l'esterno come un trasmettitore wireless o un collegamento via cavo con un altro dispositivo. Il problema principale che si presenta nell'uso di questo keylogger sta nel fatto che è facilmente individuabile osservando i connettori sul retro del computer: a meno che non si tratti di un PC che non disponga di facile accesso al retro, è evidentemente difficile riuscire a installarne uno o per lo meno fare in modo che non venga scoperto. Negli ultimi tempi, però, l'interfaccia PS/2 sta cadendo sempre più in disuso, soppiantata progressivamente dalle tastiere USB o wireless (che passano comunque via USB). Esiste comunque una possibilità di usare un keylogger hardware: si tratta di un dongle USB (ma in alternativa all'USB si può usare qualunque altro collegamento, come la porta seriale o la porta parallela) che, opportunamente pilotato da driver software, può compiere ugualmente il proprio compito di spione.

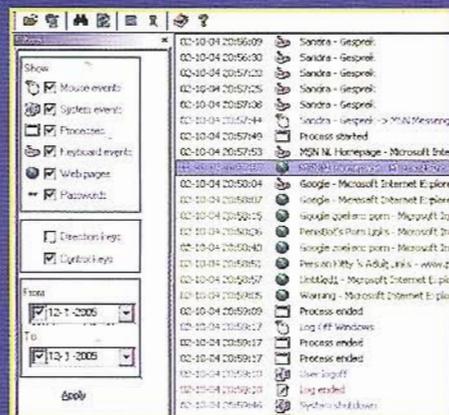
La schermata del pannello di controllo di un keylogger software.

È superfluo dire che, oltre a permanere il rischio di individuazione qualora chi usi il PC possa controllarne i connettori sul retro, in questo caso è presente anche un rischio relativo all'individuazione del software. Esistono tecniche per nascondere i processi e i driver in esecuzione sul computer dai metodi di individuazione normali (come il Task manager di Windows), ma software opportunamente costruito può rilevarli e segnalarli alla vittima.
In entrambi i casi, dongle su PS/2 oppure su altro tipo di connettore, basta un'occhiata al retro del computer per individuarlo e rimuoverlo: la miglior difesa quindi è costituita dal rendere sempre e facilmente accessibile il retro del nostro computer quando altre persone possono usarlo in nostra assenza.

:: Tipo 2: software

Il secondo tipo di keylogger è costituito semplicemente da software opportunamente scritto per intercettare i segnali della tastiera. Per funzionare, un software di questo tipo deve necessariamente inserirsi in qualche modo nella catena di comunicazione delle informazioni che va dalla tastiera stessa al kernel del sistema operativo che deve processare i segnali. Per esempio, può inserirsi prima del driver software della tastiera, intercettandone i segnali, registrandoli in un log di qualche tipo (file di testo o invio diretto via connessione a Internet) e lasciandoli poi scorrere per il percorso normale in modo che l'utente non si accorga dell'intrusione. Addirittura, alcuni tipi di keylogger sono in grado di catturare schermate di quanto accade sul PC, in forma di immagini statiche o di video.

Zemana AntiLogger è un software di protezione commerciale in grado di bloccare molti keylogger, ma non tutti.

Fermo restando che questi software usano tutti tecniche stealth per non essere individuati se non mediante opportuni strumenti, va notato che sono costretti a lasciare una traccia nel sistema su cui vengono installati: devono essere presenti uno o più file che vengono avviati dal sistema durante il boot, i meno evoluti salvano in locale testi e immagini che costituiscono il log e quelli che trasmettono direttamente i log via Internet o connessione di rete causano occupazione di banda che può risultare sospetta agli occhi di chi in quel momento non sta usando browser, client email o altri programmi di comunicazione. Se non si è sufficientemente accorti in termini di sicurezza del proprio sistema, questi keylogger risultano un osso duro da scovare e da rimuovere. Gli antivirus in grado di rimuovere il malware possono riconoscere i più diffusi, ma poco possono per quelli di nuova concezione che hanno così il tempo sufficiente per rubarci password o numero di carta di credito. Esistono sistemi per ingannarli, ma poco pratici: per esempio l'uso di una tastiera virtuale (come quella di Accesso facilitato di Windows) da usare col mouse, ma nulla vale come tenere gli occhi bene aperti e le difese sempre alte.

Deep Security Auditing con Lynis

La sicurezza di un'infrastruttura IT è un processo che parte dalle fondamenta: vediamo come

Quando ci si accinge a verificare lo stato di sicurezza di un sistema informatico, sono molte le variabili che devono

Figura 1: La fase di inizializzazione di Lynis offre un quadro preliminare per la formulazione del report, avendo cura di evidenziare gli aspetti salienti del sistema.

```
    - SSH option: Protocol...                                  [ OK ]
    - SSH option: StrictModes...                               [ OK ]
    - SSH option: AllowUsers...                                [ NOT FOUND ]
    - SSH option: AllowGroups...                               [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] SNMP Support
------------------------------------
  - Checking running SNMP daemon...                            [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Databases
------------------------------------
  - MySQL process status...                                    [ NOT FOUND ]
  - PostgreSQL processes status...                             [ NOT FOUND ]
  - Oracle processes status...                                 [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] LDAP Services
------------------------------------
  - Checking OpenLDAP instance...                              [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Software: PHP
------------------------------------
  - Checking PHP...                                            [ FOUND ]
  - Checking PHP disabled functions...                         [ FOUND ]
    - Checking register_globals option...                      [ OK ]
    - Checking expose_php option...                            [ WARNING ]
    - Checking enable_dl option...                             [ OFF ]
    - Checking allow_url_fopen option...                       [ ON ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]
```

Figura 2: Il processo di auditing di Lynis è modulare, per ogni sezione d'analisi è offerto un chiaro resoconto delle criticità rilevate.

essere prese in considerazione. Malgrado la naturale evoluzione dei sistemi operativi e degli applicativi software sia un processo volto a migliorare in modo concreto l'esperienza in termini di qualità e sicurezza percepita dall'utente, spesso vi sono determinate azioni, dimenticanze, errori che vanificano di fatto le migliorie apportate al software da parte dei produttori. Per rendere maggiormente chiaro ciò a cui ci riferiamo, consideriamo, per un attimo, l'impatto che avrebbe, ad esempio, un'errata configurazione di un server FTP qualora un utente anonimo avesse gli stessi privilegi in lettura ed in scrittura, relativamente ad una stessa directory, rispetto ad un utente autorizzato. Sebbene questo sia un esempio estremamente generalizzante, è facile intuire che, per quanto l'adozione di sistemi estremamente moderni, efficienti e sicuri possa andare, per certi versi, a limitare eventuali danni imputabili ad errori architetturali presenti nel software, riuscire ad individuare eventuali bug dovuti alla cattiva implementazione di un servizio in termini di configurazione del medesimo è piuttosto difficile.

L'auditing di un sistema informatico o, più in generale, di un'infrastruttura IT, deve necessariamente tener conto di alcuni aspetti che prescindono dal software fine a se stesso; deve pertanto essere un processo che possa offrire un quadro di insieme dell'environment entro cui operiamo al fine di ridurre al minimo il rischio che determinate "distrazioni" possano tradursi nell'esposizione dei nostri servizi a vulnerabilità del tutto inaspettate.

Naturalmente, è pressoché impossibile determinare a priori se sono stati commessi errori di configurazione di un sistema, soprattutto quando si ha a che fare con una varietà estesa e distinta di sistemi operativi e quando, per ognuno di essi, i file e le metodologie per configurare i servizi cambiano. In tale ottica, pertanto, sarebbe particolarmente utile avvalersi di strumenti capaci autonomamente di effettuare quelle che possono considerarsi le operazioni di prassi all'insegna di un'accurata analisi dall'interno di un sistema informatico.

In linea del tutto generale, offrire risposta a determinati interrogativi quando si ha a che fare con una moltitudine di OS può essere un'operazione che richiede del tempo e che spesso offre risultati direttamente proporzionali alle abilità del sistemista ed all'esperienza maturata da quest'ultimo nel corso del tempo. Risulta quindi chiaro come tutti possano trarre dei benefici dall'avere un tool che si preoccupi di determinare in maniera del tutto automatizzata ed in base al sistema operativo entro cui viene adoperato, quando il sistema è stato installato e quali patch sono state implementate, se e come sono stati organizzati file e permessi, a quali dipendenze deve rispondere il sistema, chi ha accesso a file di sistema e con quali privilegi, quali software accedono a

SISTEMI OPERATIVI SUPPORTATI DA LYNIS

Arch Linux, CentOS, Debian, Fedora Core 4 e successive, FreeBSD, Gentoo, Knoppix, Mac OS X, Mandriva 2007, OpenBSD 4.*, OpenSolaris, OpenSuSE, PcBSD, PCLinuxOS, Red Hat - RHEL 5.*, Slackware 12.1, Solaris 10, Ubuntu.

ALCUNI DEI TEST EFFETTUATI DA LYNIS

- **Lettura ed analisi delle informazioni di rete;**
- **analisi dei file di configurazione relativi ai servizi attivi sull'host;**
- **verifica di software datato e/o vulnerabile;**
- **analisi dei sistemi di logging;**
- **analisi della configurazione del firewall di sistema;**
- **controllo privilegi, permessi dei file ed account utenti;**
- **controllo dei certificati SSL scaduti.**

determinate aree riservate del sistema, quali file di configurazione sono scritti in modo corretto e quali no e che il livello di esposizione complessivo presenta il sistema. A rispondere ai nostri interrogativi ci pensa Lynis, un software open source, forse ai più sconosciuto, ma che, rivolgendosi a network e system administrator, consulenti di sicurezza e penetration tester consente, attraverso un'analisi di tipo host based, di valutare il fattore di rischio a cui è esposta la nostra infrastruttura IT.
La metodologia con la quale Lynis conduce l'auditing del nostro sistema trae naturalmente vantaggio dal fatto che essa è eseguita internamente all'host e che quindi l'applicativo gode di pieno accesso al sistema locale, potendo espletare le sue funzioni avvalendosi di un quantitativo di informazioni decisamente maggiore rispetto ad un auditing tool di tipo network based.
Nulla ci vieta, ovviamente, di combinare questo genere di analisi a quella effettuata da altri applicativi di altra natura massimizzando, di fatto, il risultato in termini di completezza e riducendo al minimo il fattore di rischio.
Resta inteso che Lynis non è un software per hardenizzare il nostro sistema; esso infatti non modificherà in alcun punto il nostro OS bensì si limiterà ad offrire un report abbastanza esaustivo dello stato di sicurezza del sistema lasciando a noi il compito di individuare ed adottare le soluzioni che meglio si adattano ai rischi eventualmente individuati.
Il lavoro che il programma svolge varia da PC a PC, adattandosi al sistema operativo rilevato. Un elenco di OS supportati ed alcuni dei test svolti da Lynis è possibile leggerli negli appositi box. In ogni caso il sito web a cui fare riferimento per eventuali aggiornamenti è www.rootkit.nl/projects/lynis.html. L'autore di Lynis è un volto ampiamente conosciuto nel panorama del free software ed abbiamo avuto modo di conoscerlo in HJ 190; stiamo parlando di Michael Boelen: noto esperto di sicurezza in ambito UNIX nonché autore del famosissimo tool "Rootkit Hunter" e di svariati script molto utili quando si ha a che fare con la stragrande maggioranza delle distribuzioni Linux ed in generale con sistemi di tipo unix-like.
Al momento della scrittura di questo articolo l'ultima versione di Lynis disponibile per il download è la 1.2.7 rilasciata il 1 Novembre 2009 le cui novità sono visibili attraverso il changelog ufficiale del progetto all'indirizzo www.rootkit.nl/files/lynis-changelog.html.

:: Installazione e aggiornamento di Lynis

Lynis è sviluppato in shell scripting; questo rende di fatto l'installazione dello stesso non necessaria e consente l'esecuzione del software anche da dispositivi rimovibili e supporti esterni.
Qualora volessimo comunque mantenere una copia locale dell'applicativo per utilizzarlo quando ve ne sia necessità o, magari, per renderlo un processo schedulato nella nostra crontab, procederemo come di seguito.
Prima di tutto creeremo una directory che conterrà tutti i file di Lynis, scaricheremo pertanto l'archivio contenente l'applicativo all'interno di quest'ultima, lo scompatteremo, consentiremo l'esecuzione del file lynis.sh e infine, creeremo un link all'eseguibile nella binary path del nostro sistema. Da shell, con i privilegi di root, pertanto, digitiamo:

```
# mkdir /usr/local/lynis
# cd /usr/local/lynis
# wget http://www.rootkit.nl/files/lynis-1.2.7.tar.gz
# tar zxvf lynis-1.2.7.tar.gz
# cd lynis-1.2.7; chmod +x lynis.sh
# ln -s lynis.sh /usr/local/bin/lynis.sh
```

Da questo momento Lynis sarà dispo-

```
-[ Lynis 1.2.7 Results ]-

Tests performed: 134
Warnings:
----------------------------
 - [02:45:06] Warning: No password set on GRUB bootloader [test:BOOT-5121] [impact:M]
 - [02:45:10] Warning: iptables module(s) loaded, but no rules active [test:FIRE-4512] [impact:L]
 - [02:45:10] Warning: Root can directly login via SSH [test:SSH-7412] [impact:M]
 - [02:45:11] Warning: PHP option expose_php is possibly turned on, which can reveal useful information for attackers. [test:PHP-2372] [impact:M]
 - [02:45:11] Warning: No running NTP daemon or available client found [test:TIME-3104] [impact:H]

Suggestions:
----------------------------
 - [02:45:06] Suggestion: Run grub-md5-crypt and create a hashed password. After that, add a line below the line saying timeout=<value>: password --md5 <password hash> [test:BOOT-5121]
 - [02:45:07] Suggestion: Install a PAM module for password strength testing like pam_cracklib [test:AUTH-9262]
 - [02:45:07] Suggestion: When possible set expire dates for all password protected accounts [test:AUTH-9282]
 - [02:45:07] Suggestion: Configure password aging limits to enforce password changing on a regular base [test:AUTH-9286]
 - [02:45:07] Suggestion: To decrease the impact of a full /home file system, place /home on a separated partition [test:FILE-6310]
 - [02:45:07] Suggestion: To decrease the impact of a full /tmp file system, place /tmp on a separated partition [test:FILE-6310]
 - [02:45:08] Suggestion: The database required for 'locate' could not be found. Run 'updatedb' or 'locate.updatedb' to create this file. [test:FILE-6410]
 - [02:45:08] Suggestion: Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [test:STRG-1840]
 - [02:45:08] Suggestion: Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft [test:STRG-1846]
 - [02:45:10] Suggestion: Disable iptables kernel module if not used or make sure rules are being used [test:FIRE-4512]
 - [02:45:11] Suggestion: Change the expose_php line to: expose_php = Off [test:PHP-2372]
 - [02:45:11] Suggestion: Change the allow_url_fopen line to: allow_url_fopen = no, to disable downloads via PHP [test:PHP-2376]
 - [02:45:11] Suggestion: Enable auditd to collect audit information [test:ACCT-9628]
 - [02:45:11] Suggestion: Check if any NTP daemon is running or a NTP client gets executed daily, to prevent big time differences and avoid problems with services like kerberos, authentication or logging differences. [test:TIME-3104]
 - [02:45:12] Suggestion: Harden the system by installing one or malware scanners to perform periodic file system scans [test:HRDN-7230]
================================================================
Files:
 - Test and debug information      : /var/log/lynis.log
 - Report data                     : /var/log/lynis-report.dat
================================================================
Hardening index : [48]     [#########          ]
================================================================
Lynis 1.2.7
Copyright 2007-2009 - Michael Boelen, http://www.rootkit.nl/
================================================================
```

Figura 3: I report dell'analisi effettuata evidenzia tutte le potenziali vulnerabilità rilevate, eventuali suggerimenti di sicurezza e l'indice di hardening del nostro sistema. In questo caso abbiamo totalizzato uno score di 48/100.

nibile in modo definitivo sul nostro PC e richiamabile, da root, attraverso il comando “lynis” qualunque sia il percorso dove ci troviamo. Sarà inoltre sempre possibile controllare se vi siano aggiornamenti disponibili per l’applicativo attraverso il comodo comando “lynis --check-update”.

Segnaliamo inoltre che Lynis è disponibile anche in forma pacchettizzata per diverse distribuzioni Linux.
Per Debian, ad esempio, è disponibile l’apposito pacchetto per tutti e tre i rami della distro (stable: lynis 1.1.7, testing: lynis 1.2.7, sid: lynis 1.2.7). In questo caso sarà sufficiente digitare da shell “apt-get install lynis” affinché sul nostro PC venga installata la versione più aggiornata dell’applicativo relativa al repository debian utilizzato.

:: Avvio del processo di analisi

Per testare l’operato di Lynis abbiamo utilizzato un’installazione standard di Debian testing corredandola di alcuni pacchetti di uso comune quali php5, apache 2, iptables ed openSSH. Per avviare il processo di auditing dell’intero sistema in modo interattivo è sufficiente digitare da shell con privilegi di root:
 # lynis -c

A questo punto, il software suddividerà l’insieme dei test effettuati per categorie; terminato ogni blocco di analisi sarà richiesta la pressione del tasto Invio per proseguire con il successivo. È possibile, in ogni caso, evitare questa interazione specificando l’opzione “-Q” (quick) come argomento.

```
debby:/home/giovanni# lynis --tests-category php

[+] Software: PHP
------------------------------------
  - Checking PHP...                                    [ FOUND ]
  - Checking PHP disabled functions...                 [ FOUND ]
    - Checking register_globals option...              [ WARNING ]
    - Checking expose_php option...                    [ WARNING ]
    - Checking enable_dl option...                     [ OFF ]
    - Checking allow_url_fopen option...               [ ON ]

  -[ Lynis 1.2.7 Results ]-

  Tests performed: 7
  Warnings:
  ----------------------------
   - [13:47:28] Warning: PHP option register_globals option is turned on, which can be a risk for variable
value overwriting [test:PHP-2368] [impact:M]
   - [13:47:28] Warning: PHP option expose_php is possibly turned on, which can reveal useful information f
or attackers. [test:PHP-2372] [impact:M]

  Suggestions:
  ----------------------------
   - [13:47:28] Suggestion: Change the register_globals line to: register_globals = Off [test:PHP-2368]
   - [13:47:28] Suggestion: Change the expose_php line to: expose_php = Off [test:PHP-2372]
   - [13:47:28] Suggestion: Change the allow_url_fopen line to: allow_url_fopen = no, to disable downloads
via PHP [test:PHP-2376]
================================================================================
```

Figura 4: Lynis consente l’analisi ristretta esclusivamente a determinati applicativi. In questo caso abbiamo dirottato la sua attenzione su PHP consci del fatto di avere la direttiva “register_globals” attiva.

Risulta utile, inoltre, la possibilità offerta dall’applicativo di poter indicare il nostro nome come auditor del sistema (**Figura 1**) attraverso l’apposito comando “-auditor ‘nostro nome’”.

Per ogni blocco di analisi effettuato saranno riportati sulla destra alcuni avvisi relativi alle criticità rilevate. Questi si suddividono in “warning” e “suggestion” stando, appunto, a significare il livello di rischio rilevato per i primi ed eventuali consigli per la configurazione dei servizi per i secondi.

Ricordiamoci sempre che, vista la natura del tool, la possibilità di ricevere falsi positivi è alta e che alcuni suggerimenti e criticità rilevate rispondono esclusivamente ad un’analisi paranoica del sistema; si lascia pertanto all’utente il necessario discernimento dei riscontri rilevati dal software.

Come visibile in **Figura 3**, al termine dei test, Lynis ci mostra un report riassuntivo marcante tutte le potenziali vulnerabilità individuate; nel nostro caso, il software ci informa, ad esempio, che sebbene sia attivo un packet filter (iptables), non risultano essere configurate alcune regole di firewalling; che è possibile loggarsi via SSH direttamente con i privilegi di root e che l’opzione expose di PHP risulta attiva, consentendo ad un eventuale attaccante la visualizzazione di informazioni sul nostro sistema. Sono infine indicati una serie di suggerimenti atti a migliorare lo stato di sicurezza generale dell’host e l’indice di hardening in base 1:100 ottenuto.

In ultima istanza segnaliamo la possibilità di concentrare l’operato di lynis solo sugli applicativi di nostro interesse, ottenendo un report relativo solo a questi ultimi; nell’esempio che segue abbiamo intenzionalmente attivato l’opzione “register_globals” di PHP (conoscendone i rischi).

Abbiamo quindi avviato Lynis con l’opzione “--tests-category php” e, coerentemente con quello che ci aspettavamo, l’applicativo ci ha informati del rischio corredando l’analisi con un opportuno suggerimento (**Figura 4**).

Giovanni Federico

REPORT QUOTIDIANI

Possiamo avviare in modo automatico la creazione di un report giornaliero attraverso l’utilizzo della crontab; per farlo creeremo un semplice cron job, del tipo:

16 6 * * * root /percorso/lynis -c –cronjob

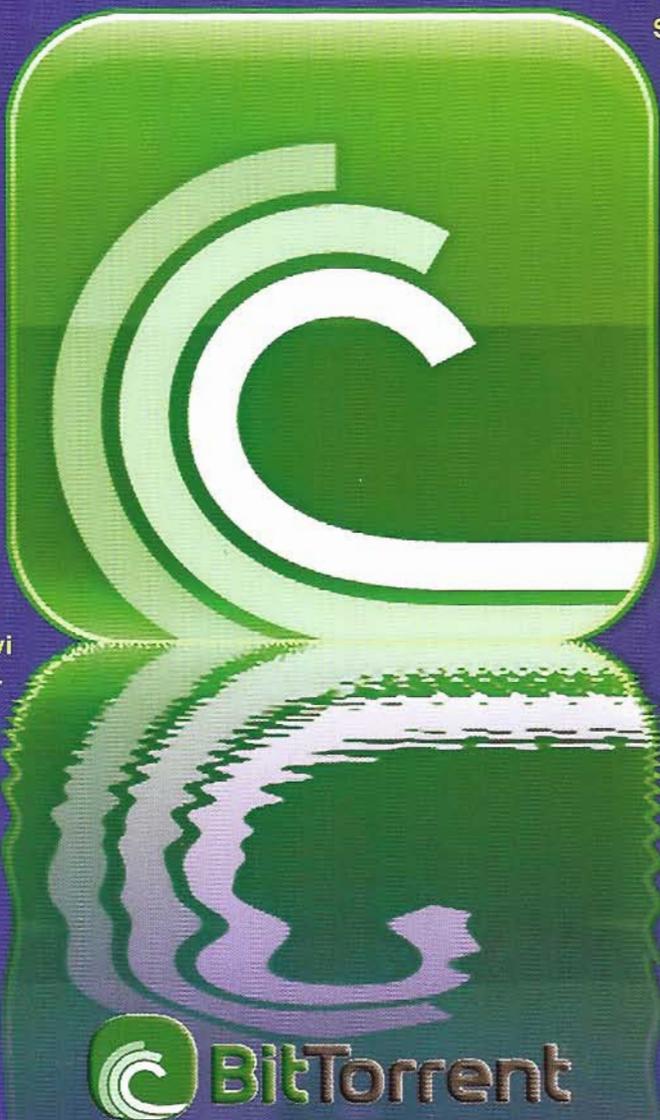
La directory dove sono contenuti sia i log del programma che i report effettuati è la classica /var/log; i file: lynis.log e lynis-report.dat.

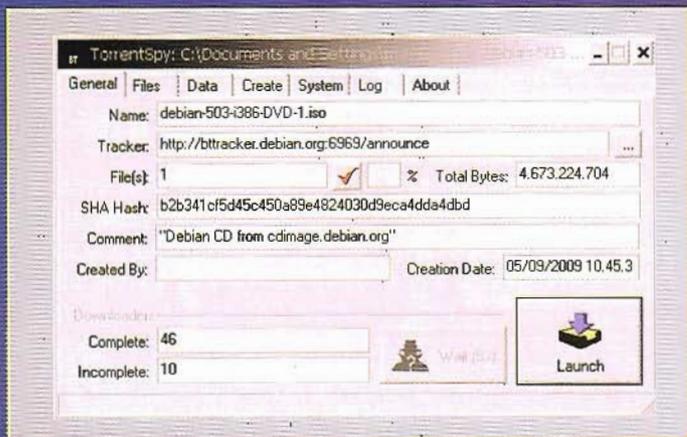
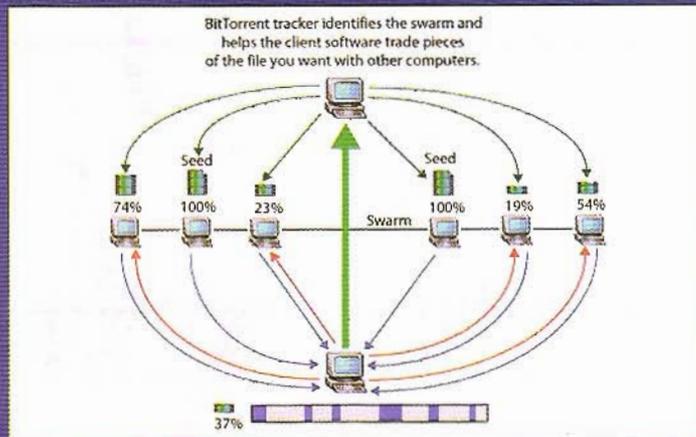
Analisi dei torrent

Cosa si nasconde all'interno del "fiume di bit" più famoso della Rete

Siamo abituati a scaricare abitualmente file dalle reti torrent e l'unica cosa che ci preoccupa è se ci sono o no seeds. Ma un file torrent è solo la punta di una piramide di informazioni nascoste che letteralmente brulicano tra i PC connessi nelle reti peer-to-peer di bittorrent, vediamo come funziona l'intero sistema.

:: Dentro il torrent

Un file torrent è un archivio binario contenente un nucleo principale costituito dall'indirizzo IP del tracker e da tutti i peer classificati attualmente come attivi (i client della rete peer-to-peer). Oltre alle informazioni di base sono presenti ulteriori dati, molto interessanti, che possiamo analizzare con tool appositi. Uno di questi è TorrentSpy (torrentspy.sourceforge.net), un tool forse un po' datato ma ancora tra i più validi. Prendiamo ad esempio il torrent relativo alla prima iso di Debian 5.0 che possiamo scaricare direttamente dal sito ufficiale (www.debian.org/CD/torrent-cd). Il programma non va installato: è sufficiente avviarlo, trascinare nella sua finestra il torrent che vogliamo studiare e potremo analizzare i dati che ci vengono mostrati.

Si distinguono chiaramente:

- il nome del file che andremmo a scaricare se lanciassimo un client torrent (nella riga Name)
- il tracker, ossia il server che il client deve interrogare per ricevere gli indirizzi cui connettersi per ricevere parti del file e che, in media una volta ogni 30 minuti, va interrogato di nuovo per aggiornarsi sui peer attivi da cui richiedere ulteriori parti
- in File vediamo quanti file sono associati al torrent e nel caso abbiamo scaricato già parte del file, cliccando sulla V possiamo chiedere al software di dirci se abbiamo il totale o solo una percentuale del file completo (di cui vediamo il totale dei byte a destra)
- SHA Hash è il codice di checksum utilizzato per verificare l'integrità del torrent
- "Comment" e "Created by" sono campi descrittivi compilati da chi crea il torrent, mentre "Creation Date" corrisponde alla data esatta della creazione dell'archivio
- In Complete/Incomplete possiamo vedere la situazione corrente di quanti hanno già scaricato il file e possono quindi ritrasmetterlo (Seeders); questa informazione può essere aggiornata se siamo connessi e clicchiamo su Update

In questa finestra appaiono una serie di informazioni sostanzialmente analoghe a quelle fornite da un client come BitTorrent.

Schema riepilogativo del funzionamento del protocollo torrent e della tecnica di swarming.

:: Il protocollo torrent

Tipicamente il file da scaricare viene scomposto in parti uguali di 256Kb l'una (dette chunk) che vengono scambiate continuamente tra tutti i client connessi allo stesso tracker in modo da replicare il file all'interno di questa sottorete. Questa tecnica prende il nome di swarming (brulicare), il che rende bene l'idea del movimento di bit che si genera, ma soprattutto spiega come sia possibile ottenere un download parallelo: in pratica attivando una connessione dal client verso diversi nodi della rete peer-to-peer, si riescono a scaricare piccole parti da diversi indirizzi sfruttando pienamente la banda a disposizione. In questo modo si ricevono in contemporanea diversi segmenti del file che man mano verrà completato. Ogni volta che il client riceve per intero un chunk, informa tutti i client cui è connesso dell'aggiornamento avuto.

L'elenco completo dei file inclusi nel torrent compare nella seconda finestra "Files".

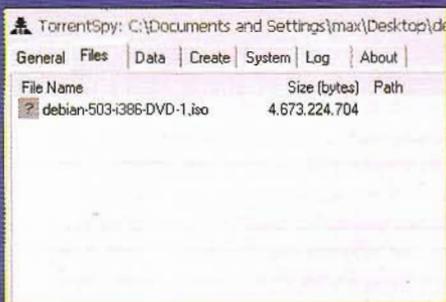
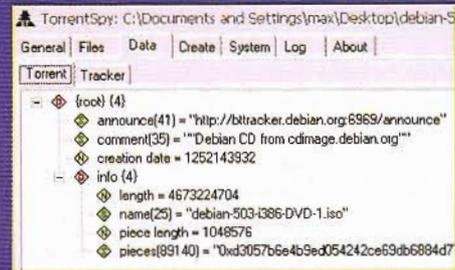
La politica di scambio dati tra client segue due linee guida:

- prima di tutto, vengono preferiti gli scambi verso un client che già ci sta mandando dei chunk, tecnica denominata tit-for-tat volta a stimolare la condivisione dei file piuttosto che il solo download a senso unico
- secondariamente, ogni peer limita il numero di peer che può servire a 4 e monitora costantemente quali sono i migliori 4 downloader (in termini di byte al secondo scambiati) nel caso si tratti di un seed, o dei 4 migliori uploader nel caso si tratti di un leecher

Queste linee guida sono state implementate in BitTorrent il quale, per limitare i download nel caso di sovraccarico, rifiuta il collegamento di ulteriori downloader mentre sta trasferendo i chunk; ogni 10 secondi circa campiona i trasferimenti in corso e nel caso trovi connessioni migliori, appena possibile accetta quelle più prestanti per il download.
Oltre a queste politiche di tipo "statico", vengono applicate delle politiche di tipo euristico che ogni 30 secondi prevedono di rischiare su una connessione nuova, tagliando una di quelle presenti a prescindere dalla velocità rilevata. In particolare, la scelta dei chunk da scaricare è basata sulla massima entropia realizzabile che permette di avere il file il più possibile diffuso all'interno della rete peer-to-peer. Questa tecnica prende il nome di rarest-first-policy e prevede che il chunk meno diffuso sia il primo ad essere duplicato. C'è un'eccezione prevista, che si realizza quando si connette un nuovo client che non ha alcun chunk: in questo caso, dato che non può attendere di ricevere il chunk più raro, viene scelto in modo casuale quale chunk ricevere per primo dopodiché si abilita la rarest-first-policy.

:: Considerazioni

A prescindere dalle polemiche relative al download di materiale protetto da copyright, leggi e leggine, non si può non riconoscere che il protocollo stesso sia un'opera di ingegno affascinante ed efficiente e che invece di limitarne l'uso sarebbe utile diffonderlo per ottimizzare la banda come fa da tempo la comunità OpenSource. Grazie a torrent infatti è possibile accorciare i tempi di scaricamento, nonostante le pesanti limitazioni infrastrutturali cui siamo soggetti in Italia, quindi con beneficio per tutti.

NoeXKuzE

Nelle schede di questa finestra possiamo vedere le informazioni principali contenute all'interno di un file torrent.

Indagini forensi con DEFT Linux

Questa distro Live mette a nostra disposizione strumenti avanzati per l'analisi e il recupero di sistemi

DEFT Linux è una distribuzione GNU/Linux, sviluppata in Italia, che fornisce un completo ambiente per l'analisi forense. Grazie ad essa, quindi, possiamo recuperare da un PC informazioni perse o nascoste, tentare di individuare delle password d'accesso oppure analizzare con un software di sniffing il traffico all'interno di una rete. Questa distro non deve essere installata sull'hard disk del PC su cui vogliamo effettuare le analisi: in questo modo, è possibile far uso di un ambiente d'indagine teoricamente asettico e in ciò siamo aiutati dalla scelta della distro di non montare, al momento dell'avvio, alcun dispositivo presente nel PC da analizzare, così da lasciare a noi piena libertà sugli interventi.

:: Installazione su CD e chiavetta

DEFT Linux può essere masterizzata su CD-Rom oppure trasferita su una piccola chiavetta USB. Per creare un CD di avvio apriamo con un web browser la pagina http://www.deftlinux.net/download e clicchiamo sul link di uno dei mirror disponibili e scarichiamo il file deftv5.iso. Al termine del download masterizziamo questo file, che contiene l'immagine ISO del CD di avvio di DEFT Linux 5, con un qualsiasi software di masterizzazione. La procedura per trasferire la distro su chiavetta è un po' più complicata. Avviamo un sistema Linux, ad esempio Ubuntu 9.10, ed apriamo con un web browser l'indirizzo http://www.mirrordeft.net/listing/deftpen. Quindi scarichiamo il file deftpen_5.dd. Fatto ciò, inseriamo nel nostro PC la chiavetta e individuiamo il file di dispositivo corrispondente alla chiavetta stessa: per fare questo apriamo una console di terminale e, subito dopo aver inserito la penna, lanciamo il comando dmesg. Otterremo in output il file di dispositivo della nostra penna. A questo punto, nel terminale entriamo con il comando "cd" nella directory in cui il nostro browser salva i file scaricati (lanciamo, ad esempio, "cd Scrivania"). Quindi per trasferire DEFT Linux sulla penna eseguiamo il comando seguente, inserendo al posto di /dev/sdb il file di dispositivo della chiavetta:

```
sudo dd if=Download/deftpen_5.dd
of=/dev/sdb
```

Se non usiamo Ubuntu o altre distro che utilizzano sudo per ottenere i permessi di root, eseguiamo prima il comando "su -", inseriamo la password di root e poi lanciamo "dd if=Download/deftpen_5.dd of=/dev/sdb".

```
File  Modifica  Visualizza  Terminale  Aiuto
[54927.401010] sd 10:0:0:0: [sdb] A
[54927.401018]  sdb:
[54993.876277] sd 10:0:0:0: [sdb] A
[54993.876289]  sdb: sdb1
[55100.903164] usb 1-5: USB disconn
[55103.324190] usb 1-5: new high sp
[55103.459619] usb 1-5: configurati
[55103.462290] scsi11 : SCSI emulat
[55103.462525] usb-storage: device
[55103.462530] usb-storage: waiting
[55108.460415] usb-storage: device
[55108.472121] scsi 11:0:0:0: Direc
Q: 0 ANSI: 2
```

Per trasferire DEFT Linux su una chiavetta USB dobbiamo conoscere il file di dispositivo della chiavetta: per fare questo lanciamo il comando dmesg. In questo esempio il dispositivo è /dev/sdb.

:: Avviamo DEFT Linux

Trasferita la distro nel supporto scelto, inseriamo questo nel PC da analizzare e configuriamo il BIOS per fare l'avvio dal supporto prescelto. Effettuato il boot di DEFT Linux, comparirà un menu in cui scegliere la lingua da usare: con i tasti freccia selezioniamo la voce Italiano. Nel menu di avvio della distro, quindi, scegliamo l'opzione "Start DEFT Linux v5" e premiamo Invio. Fatto ciò, verranno caricate le componenti principali del sistema operativo e comparirà il prompt dei comandi. Qui possiamo eseguire delle applicazioni a linea di comando oppure avviare l'interfaccia grafica; per fare questo lanciamo il comando "startx". e dopo qualche secondo comparirà l'interfaccia grafica di DEFT Linux, che utilizza l'ambiente desktop LXDE (http://lxde.org/). Come si è anticipato, il sistema non monta automaticamente i dispositivi presenti sul PC. Per attivare le partizioni dell'hard disk su cui vogliamo intervenire, quindi, doppiamo usare l'applicazione MountManager. Non appena avviata selezioniamo nell'elenco a sinistra la partizione da montare, poi indichiamo, a destra, il Mount point (cioè la directory in cui vogliamo che sia accessibile la partizione). Sono disponibili molte opzioni relative al mount della partizione: per accedere in sola lettura alla partizione, ad esempio, nella linguetta Ge-

neral selezioniamo per l'opzione "What users can do at this partition" il valore "Only read". Quindi nell'elenco a sinistra clicchiamo con il tasto destro del mouse sulla partizione e nel menu che appare selezioniamo la voce "Mount". Infine, per attivare la partizione clicchiamo sul pulsante Mount che a questo punto sarà comparso nella finestra.

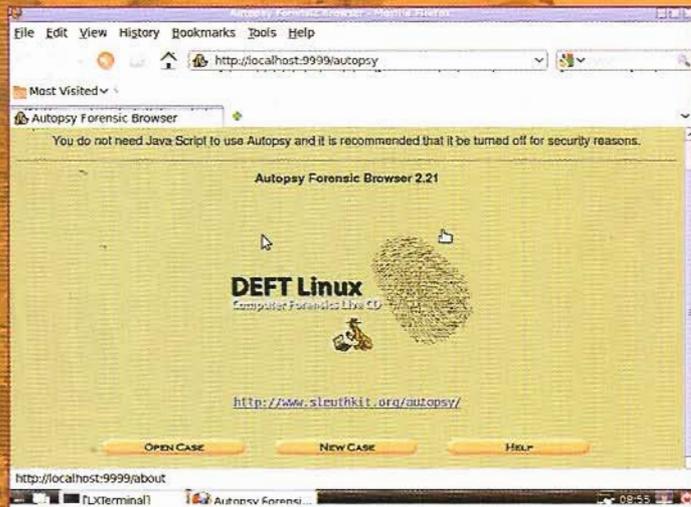
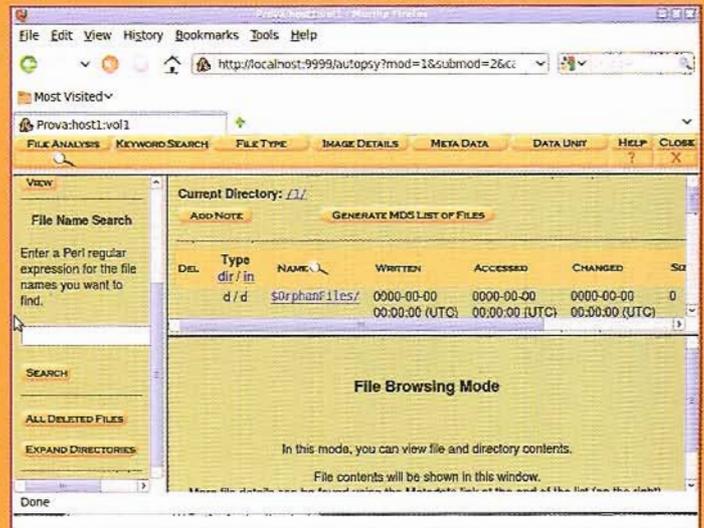
:: Autopsy e Sleuthkit

Per avviare i programmi di analisi forense forniti da DEFT Linux clicchiamo sull'icona Deft in basso a sinistra, quindi nel menu che appare entriamo nella sezione "Computer Forensic". Uno dei più importanti strumenti che questa distro mette a nostra disposizione è Autopsy, un eccellente software per le indagini digitali che permette di analizzare i dati presenti in un gran numero di filesystem (Ext2, Ext3, FAT, NTFS, UFS1 e UFS2). Autopsy non è altro che un'interfaccia grafica via web a The Sleuth Kit, un insieme di programmi a linea di comando per l'analisi forense. Vediamo, dunque, come procedere per recuperare i file cancellati da una partizione. Avviamo Autopsy cliccando sull'icona DEFT, su "Computer Forensic" e poi su Autopsy. Comparirà una finestra di terminale, in cui verrà avviato Autopsy: per chiudere il programma, quindi, basterà poi chiudere questa finestra. Dato che Autopsy utilizza un'interfaccia web, verrà avviato in automatico Firefox con aperta la URL dell'interfaccia sul PC locale (http://localhost:9999/autopsy). A questo punto, la prima operazione da compiere è creare un nuovo "caso" e fornire al programma informazioni sull'indagine forense che dobbiamo effettuare.

:: Analizziamo il disco

Per aprire un nuovo caso, nell'interfaccia di Autopsy clicchiamo sul pulsante "New Case" in basso. Quindi inseriamo nel campo "Case Name" il nome del caso da creare, mentre la compilazione degli altri campi è facoltativa. Clicchiamo poi su "New Case" in basso. Ora aggiungiamo un host, cioè un computer da analizzare: clicchiamo sul pulsante "Add Host" e nella schermata seguente diamogli un nome e clicchiamo su "Add Host". Fatto questo, dobbiamo indicare un file immagine con il contenuto del dispositivo da analizzare; in alternativa, possiamo inserire direttamente il file di dispositivo della partizione o dell'intero disco. Se vogliamo creare un file immagine lanciamo in un terminale il comando "dd" nel modo seguente, inserendo al posto di /dev/sda1 il file di dispositivo della partizione da leggere: dd if=/dev/sda1 of=sda1.dd
Al termine dell'operazione, il file sda1.dd conterrà l'immagine della nostra partizione. Nel nostro esempio, però, per semplificare utilizzeremo direttamente il file di dispositivo di una partizione. Clicchiamo quindi sul pulsante "Add Image", poi su "Add Image File". Nella schermata successiva inseriamo in Location il file di dispositivo della partizione (ad esempio, /dev/sda1) e come valore dell'opzione Type scegliamo Partition. Quindi clicchiamo su Next in basso. Nella schermata che segue possiamo lasciare i valori di default di tutte le opzioni e cliccare su Add. Se vogliamo aggiungere un altro dispositivo da analizzare clicchiamo poi su "Add Image", altrimenti clicchiamo sul pulsante OK.

:: Cerchiamo i file cancellati

Nella schermata che appare ci verrà presentato un riepilogo informativo sul dispositivo e, più in basso, un insieme di pulsanti per operare sul dispositivo stesso. Clicchiamo sul pulsante Analyze e nella schermata successiva scegliamo come metodo di analisi "File Analysis". A questo punto comparirà il contenuto della dispositivo, visualizzato come in un comune file manager. La finestra del web browser è ora ripartita in tre sezioni, più la fila di pulsanti in alto: per trovare i file cancellati entriamo nella sezione a sinistra, quella con la scritta Directory Seek, e clicchiamo sul pulsante "All Deleted Files". Nella sezione in alto a destra della finestra, quindi, verranno elencati tutti i file cancellati che sono stati individuati nella nostra partizione. Nell'elenco selezioniamo il file cancellato che vogliamo recuperare. Compariranno alcune opzioni relative al file prescelto: clicchiamo su Export per salvare il file.

La pagina iniziale dell'interfaccia web di Autopsy. Se vogliamo analizzare una partizione o un intero disco apriamo un nuovo caso cliccando sul pulsante "New Case".

Clicchiamo sul pulsante "All Deleted Files" per avere accesso ai file cancellati presenti sul dispositivo selezionato.

Qualcuno di noi conoscerà già l'ottimo servizio offerto da Evenflow Inc. chiamato Dropbox. Per tutti coloro che invece non l'avessero ancora scoperto basta dire che, grazie a un'interfaccia grafica semplice e funzionale, viene reso disponibile anche ai meno "smanettoni" un sistema di sincronizzazione tra le varie cartelle replicate sia su diversi PC, sia su PC e iPhone sia, ma stiamo parlando di una versione beta, anche su Blackberry. Ma non è finita qui: il bello è che il tútto è gestibile anche online tramite un qualunque browser.

:: Funzioni

Dropbox (www.Dropbox.com) è un'applicazione multipiattaforma completamente gratuita che permette di avere fin da subito 2Gb di spazio online (cui tramite un meccanismo di inviti su referral, è possibile aggiungere fino a 3Gb e raggiungere quindi i 5Gb totali) senza pagare alcun canone, che possiamo utilizzare come un hard disk virtuale costantemente sincronizzato con delle cartelle fisiche presenti nel nostro PC o nel nostro iPhone.
Per chi fosse interessato a spazi maggiori poi, sono disponibili abbonamenti mensili a partire da 9,99USD per 50Gb e 19,99USD per 100Gb. Purtroppo però per l'iPhone il limite di spazio gestibile resta comunque 2Gb proprio per un'imposizione da parte di Apple, che speriamo cambi idea visto che è una della applicazioni che aspira a diventare tra le favorite presenti in App Store. Nel caso in cui ci si stia avvicinando al limite disponibile, si viene avvisati ed è possibile guadagnare qualcosa rimuovendo i file dai preferiti (quelli segnati da una stellina).
L'applicazione una volta installata è totalmente trasparente per l'utente perché si integra nel sistema operativo monitorando una specifica cartella del filesystem (che possiamo scegliere in fase di setup o cambiare in seguito) per controllare ogni minima variazione che intervenga sui file e sulle sottodirectory. Nel momento in cui viene modificato qualcosa, viene attivata una connessione SSL verso il server di Dropbox e viene sincronizzato ciò che è cambiato. Nel contempo, nell'account online viene aggiornato il registro degli eventi e se ci sono altri PC o telefoni agganciati allo stesso account con Dropbox in funzione, riceveranno di conseguenza gli aggiornamenti dei cambiamenti effettuati non appena disponibili sul server.

Dropbox su iPhone

Come tenere costantemente sincronizzati file tra PC e iPhone

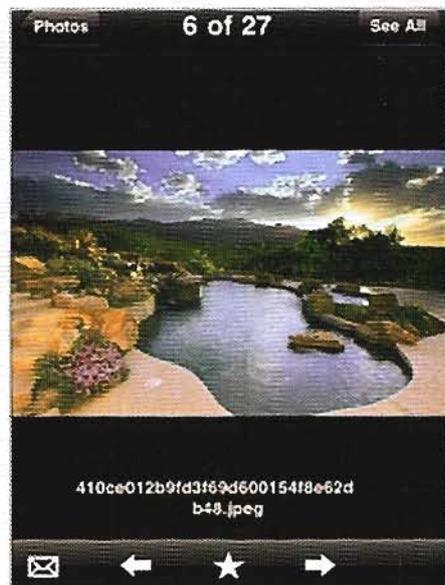
Anche se non abbiamo ancora attivato un account su Dropbox è possibile crearlo direttamente dall'installazione su iPhone.

:: Dropbox su iPhone

Per 'accesso online, l'interfaccia web standard obiettivamente un po' esosa in termini di spazio grafico viene ridotta all'essenziale (vedi all'indirizzo dropbox.com/iPhone) perché presenta per iPhone solo i controlli che permettono di scaricare i file da Dropbox direttamente sul proprio telefonino e consultare il registro degli eventi. Per quanto riguarda file come PDF e MP3, è possibile passare direttamente all'apertura e visione (e vengono anche associate graficamente le rispettive icone che ci sono familiari), mentre altri file saranno visibili solo quando si va offline andando nella cartella dei Preferiti. L'applicazione è molto ben documentata online e rende facile e divertente il suo utilizzo. Per partire subito è possibile creare un account online, scaricare l'eseguibile e lanciare l'installazione o lanciare l'installazione e scegliere la procedura guidata per creare un proprio account durante il setup. Nel caso in cui stiamo aggiungendo un altro nodo della nostra rete privata in Dropbox, basta utilizzare login e password già in possesso e vedremo che Dropbox appena installato cercherà di scaricare tutti i dati già presenti online. Occhio quindi con le connessioni a volume, nel caso si abbia qualche giga di dati da sincronizzare! Su iPhone è molto semplice fare il setup e partire con Dropbox ed è possibile aprire direttamente le foto che inseriamo. L'applicazione è reattiva, si sincronizza velocemente e non va in crash, nonostante il fatto che è stata lanciata da poco. C'è la possibilità di fare subito una foto con l'iPhone o di girare un video con l'iPhone 3GS e mandarlo immediatamente a uno dei propri contatti. Dopo l'installazione troveremo nella cartella un PDF che ci spiega il funzionamento di Dropbox su iPhone. Dal menu poi è facile scollegare il proprio iPhone ed effettuare login con un altro account nel caso lo avessimo.

:: utilizzi avanzati

Oltre a gestire un backup in tempo reale, utilissimo e alla portata di tutti quanti possono avere un accesso a banda larga, è possibile decidere di condividere i dati con altri utenti di Dropbox. Per poter attivare la condivisione, si deve agire dall'interfaccia online completa e scegliendo in Sharing il nome della cartella che sarà condivisa. Una volta creata, dobbiamo indicare gli indirizzi e-mail delle persone autorizzate ad accedere (oltre noi) che corrisponderanno ad altri account già attivi di Dropbox. Lo spazio condiviso di fatto viene tolto da quello totale fintanto che dura la condivisione. Ma grazie a questa operazione è possibile accedere liberamente ai dati condivisi da due account differenti e scambiare file tra amici. Chiaramente resteranno visibili solo i dati presenti nella cartella condivisa e solo gli utenti autorizzati potranno accedervi. Dropbox rappresenta a mio parere un servizio complementare a Gmail: se infatti con Gmail è possibile dimenticarsi dei vari problemi della posta elettronica (organizzazione, occupazione di spazio, spam, ..), con Dropbox è possibile gestire con la medesima semplicità un proprio archivio personale di dati sempre presenti, online e fisicamente su un qualunque terminale che connettiamo al server e accessibili anche dal proprio iPhone, di cui possiamo anche dimenticarci che sta funzionando perfettamente mentre lo usiamo. E anche se non lavoriamo su più macchine, ma vogliamo sempre avere a portata di mano documenti importanti da vedere ad esempio sul nostro iPhone, Dropbox diventerà un compagno insostituibile.

Una volta entrati nel nostro account possiamo controllare online tutti i file già sincronizzati in My Dropbox.

Se clicchiamo sopra un'immagine questa andrà direttamente nel viewer come se Dropbox non ci fosse.

Massimiliano Brasile